World Law Group

Global Guide to Whistleblowing Programs 2016

www.theworldlawgroup.com

WORLD LAW GROUP GLOBAL GUIDE TO WHISTLEBLOWING PROGRAMS, 2016

Please note that this guide provides general information only. Its purpose is to provide a brief overview of legislation governing whistleblowing programs in each jurisdiction covered. This information is not comprehensive and is not intended as professional or legal advice, generally or in a given situation. This guide is an outline of country-specific obligations, which may change. Facts and issues vary by case. Legal counsel and advice should routinely be obtained, including locally for any particular jurisdiction. Please consult your own counsel.

CONTENTS

I. INTRODUCTION

Companies acting in a global environment with subsidiaries and businesses across a large number of jurisdictions face a daunting task: establishing compliance guidelines and whistleblowing reporting schemes that are both effective and consistent across the entire organization and which, at the same time, observe applicable data protection, privacy and labour laws in many countries. The aim of this publication is to provide a dedicated resource on this subject, distilling the experience of numerous World Law Group ("WLG") firms into a single reference.

In an environment where adherence to anti-corruption, anti-bribery, fraud, and money-laundering laws is increasingly important, the structuring of whistleblowing programs has become more complex and the subject of regulation. Some laws, like the Sarbanes-Oxley Act ("SOX") in the United States, require such reporting mechanisms, while others, such as the Foreign Corrupt Practices Act ("FCPA") and Dodd-Frank Act in the U.S., and the United Kingdom's Bribery Act, encourage internal reporting programs of this sort.

A SOX hotline procedure for European operations and separate country notices for employees, translated into local languages, are employed by some multinational companies. These are usually done in a manner so as not to disturb the underlying code of conduct or business ethics. Third-party hotline providers help with the solution but companies also have additional, independent obligations.

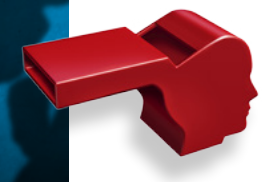
The aim of this publication is to make the understanding and, we hope, the execution of that process easier. Our goal, accordingly, is to facilitate a framework for analyzing and constructing multinational or global whistleblowing programs, with an eye towards consistency, where possible, and adherence to local law. Whether developments like the new EU General Data Protection Regulation, which is to enter into force in 2018, will simplify this process, remain to be seen.

This guide focuses on relevant laws around the world as they stand in mid-2016. However, change in this area is constant so we encourage you to consult additional references.

We hope you find this guide useful.

Mark E. Schreiber
Chair, WLG Privacy & Data Protection Group
Locke Lord LLP
Boston, Massachusetts, U.S.A.
Email: mark.schreiber@lockelord.com
Tel: + 1 617 239 0585

Christian Runte
Co-Chair, WLG Privacy & Data Protection Group
CMS Germany
Munich, Germany
Email: christian.runte@cms-hs.com
Tel: + 49 89 238 07163



Note regarding European Law and Privacy Shield

Please be aware that we have added a new section on the European Union. In the future, personal data protection law in Europe will be harmonized. As of 2018, the General Data Protection Regulation will replace the current European Data Protection Directive (and the implementing national laws). This is referenced in the individual EU country chapters of this guide.

Also, the new Privacy Shield, replacing the Safe Harbour for personal data transfers from EU and EEA countries (and eventually Switzerland) to the US, has now been finalized and approved. It will go into effect August 1, 2016 for new applications. Any discussion of the implications and mechanics of the Privacy Shield for whistleblowing schemes is beyond the scope of this publication and will have to wait for a later day.

Acknowledgments

This guide would not have been possible without the extraordinary contributions of many lawyers and others from a number of World Law Group member firms. Several individuals deserve special recognition for the painstaking effort and careful attention that such a global publication requires. For this edition, Sarah Haghdoust, a Senior Associate at CMS Germany in Munich, worked tirelessly in the compilation and organization of the various country contributions of the many WLG firms. Julie Engbloom, a partner in Lane Powell PC in Portland, Oregon, along with attorneys Laura L. Richardson, Cozette Tran-Caffee and Hans N. Huggler in that firm handled the legal review.

Shelley Boyes, the World Law Group's Director of Marketing & Communications, kept us on track (a not easy task) and managed final proofing, copy-editing and production.

The World Law Group is exceedingly grateful for the truly hard work, fine efforts and determination of all of these individuals and firms in helping us see this project through to conclusion.

II. ABOUT THE WORLD LAW GROUP

The World Law Group is a network of 54 leading independent law firms with more than 350 offices in major commercial centres worldwide. WLG member firms comprise approximately 18,000 lawyers working in a comprehensive range of practice and industry specialties. Clients can access local knowledge and seamless multinational service via a single call to any World Law Group member firm.

A directory of all WLG member firms and their respective Key Contact Partners is available at www.theworldlawgroup.com. If jurisdictions relevant to your organization are not included in this guide, WLG members can usually provide contacts for those purposes.

For more information, visit www.theworldlawgroup.com.

About the WLG Privacy & Data Protection Group

The World Law Group's Privacy & Data Protection Group is made up of lawyers in the WLG's member firms worldwide who have data protection, privacy and related compliance work as a focus of their practice, both in their countries and globally. The group's goal is to enhance the provision of relevant and seamless client services, including advising on cross-border data transfers, privacy risk assessments and data breach services to multinational entities, and to develop proactive compliance procedures and techniques in this increasingly demanding field.

Group members from around the world meet by teleconference and at many World Law Group semi-annual conferences to exchange information about emerging privacy issues and challenges for multinational and local country clients, and to work together on various projects. Group members have collaborated on several noteworthy publications, both online and in print, and have organized numerous webinars and other information events for members and clients.

Members have also recently collaborated to produce an expanded and updated second edition of the well-regarded *WLG Global Guide to Data Breach Notifications*, which can be downloaded from its companion website, www.globaldatabreachguide.com.

1. ARGENTINA

1.1 Applicable law and/or data protection guidelines?

Argentina has no specific whistleblower protection laws in place. However, there are labour laws, constitutional and data protection laws ("DPL") and case law that provide certain guidelines, although these do not directly address the issue. In particular, each company implementing a whistleblower program must comply with the DPL when a database with personal information is created.

These whistleblowing programs must not violate or infringe labour laws and regulations, including but not limited to collective bargaining agreements and benefits awarded previously to the employees.

1.2 Is an English translation available?

Yes, an unofficial translation of the Personal Data Protection Act is available:

unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan044147.pdf.

1.3 Is prior notification or approval required?

Companies must always notify their employees before the implementation of a whistleblower program. However, it is not necessary to notify the Data Protection Authority ("DPA") or seek approval from any agency or authority.

Nevertheless, if the whistleblower program includes the creation of a database with personal information of the employees, the company must register the database in accordance with the DPL.

1.4 Can notification or approval be filed online?

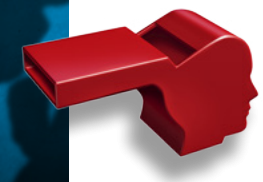
The forms to register the database are generated online but their originals have to be submitted to the DPA.

1.5 Generally, how long does it take to get approval?

The database is generally registered by the DPA within 72 hours after the submission of the completed original forms, if there are no concerns.

1.6 Contact information for Data Protection Authority?

Name:	Dirección Nacional de Protección de Datos Personales
Address:	Sarmiento 1118 – 5º Piso; Ciudad Autónoma de Buenos Aires; Buenos Aires, Argentina (C1041AAX)
Telephone:	+54 11 4383-8512 / 8510 / 8513 / 8514 / 8521
Email:	infodnpdp@jus.gov.ar
Website:	www.jus.gov.ar/datos-personales.aspx



1.7 What is the scope of reporting permitted?

There is no limit to the scope permitted for reporting in whistleblowing programs in Argentina (audit, financial matters, bribery, corruption, discrimination, etc.) as long as it does not concern facts about the employee that are beyond the scope of their employment, bearing in mind that the dignity and privacy of employees should be protected at all times.

No person may be required to disclose personal information revealing racial or ethnic origin, political views, religious beliefs, philosophical or moral stands, union affiliations or any information referring to health or sexual life (i.e., "Sensitive Data").

1.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No, companies are free to decide who can make a report under a whistleblowing program.

1.9 Are there limits on who can be a subject of a report?

No. However, it is advisable to include the complete staff (even the managerial staff), in order to avoid discrimination claims.

1.10 Is anonymous reporting permitted?

Yes, whistleblower programs may allow anonymous reporting. The company must, however, obtain the information legally and guarantee the accused employee's right to be heard, and ensure the case is dealt with fairly.

1.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes. According to Section 11 of the DPL, and its Regulatory Decree 1558/2001, personal data may only be transferred in compliance with legitimate interests of the transferring and receiving parties, and, generally requires the prior consent of the data subject, which may be later revoked.

Consent to the transfer of personal data is not required when:

(a) A law so provides;

(b) The information is obtained from public sources;

(c) The transfer is made between government agencies in the exercise of their respective duties;

(d) The information only includes name, ID, Tax ID, occupation, birth date and address;

(e) The information is collected due to a contractual, scientific or professional relationship with the data subject, and is necessary for its development;

(f) In financial entities' operations and their customers' data according to section 39 of Law 21,526;

(g) The transfer is made directly between governmental agencies;

(h) The data relates to health issues, and is used for emergencies, epidemiologic studies or other public health purposes, provided that the identity of the subject is protected; or

(i) The data has been de-identified (anonymized) such that it may no longer be linked with the corresponding subjects.

According to Section 12 of the DPL, and its Regulatory Decree 1558/2001, the transfer of any personal information to countries or international or supranational entities that do not provide adequate levels of protection is prohibited.

The prohibition on transferring data shall not apply in certain cases. Among the most common exceptions are:

(a) The data owner gives his/her express consent. (This consent will not be necessary if the transfer of data is through a public registry legally authorized to facilitate information to the public);

(b) International judicial cooperation;

(c) Exchange of medical information, when so required for the treatment of the party affected, or in case of an epidemiological survey, provided that a disassociation procedure was made to prevent the identification of individuals involved; and

(d) Stock exchange or banking transfers, in connection with their related transactions, and in compliance with applicable law.

On March 6, 2003, Argentina became the first Latin American country to receive the EU Data Protection Working Party's approval for its data protection framework. The adequacy finding means that data can be freely transferred between EU member states and Argentina without fear of violating the EU Data Protection Directive.

1.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

Prior written consent of employees is required to: a) create a database with their personal information, except the data that is necessary for the development of the labour relationship, and b) transfer the above-mentioned information to a third party with the exemptions mentioned in 1.11. If the whistleblower program does not include the creation of a database, the company still must notify the employees prior to its implementation. Usually, those programs are included in the organization's "Ethics Code" or "Standard Operating Procedures" or in another company policy.

1.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

No, there is no need for consultation with a Works Council or any union or other employee representative group for the implementation of whistleblowing programs.

1.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

Although there are no specific requirements for the implementation of a whistleblower program, both the DPL and its Regulatory Decree 1558/2001 establish a general obligation to place data security controls on data processors.

Section 9 of the DPL establishes that the person responsible for, or the user of, data files must take such technical and organizational measures necessary to guarantee the security and confidentiality of personal data, in order to avoid its alteration, loss, unauthorized consultation or treatment, and which allow for the detection of any intentional or unintentional distortion of such information, whether the risks arise from human conduct or the technical means used.

Moreover, Section 9 provides that it is prohibited to record personal data in files, registers or banks that do not meet the requirements of technical integrity and security.

The material must be deleted once used for the purpose for which it was collected.

For more information, contact:

Name: Pedro Mazer or Paola Trigiani
Firm: Alfaro-Abogados
Address: Avenida Del Libertador 498, Floor 3°, Buenos Aires, Argentina
Telephone: +54 11 4393 3003
Fax: +54 11 4393 3001
Email: pmazer@alfarolaw.com or ptrigiani@alfarolaw.com
Website: www.alfarolaw.com

2. AUSTRALIA

2.1 Applicable law and/or data protection guidelines?

Australia has specific whistleblower protection laws in place to encourage and protect disclosures of wrongdoing both in the public and private sectors, but they are rarely used and often are criticized as being ineffective.

Public Sector

In terms of the public sector, each State and Territory in Australia has enacted legislation to protect the identities of individuals who make disclosures in the public interest[1].

These statutes provide protection to individuals who disclose improper conduct of public officers and public bodies, and also provide for the disclosed matters to be properly investigated.

The Public Interest Disclosure Act 2013 (Cth) provides similar protections at a Commonwealth level for public officials to report suspected wrongdoing.

Private Sector

In the private sector, corporate whistleblowers are afforded protection under Part 9.4AAA of the Corporations Act 2001 (Cth). The legislation protects whistleblowers who make good-faith disclosures of suspected contraventions of that Act to the Australian Securities & Investment Commission ("ASIC") or the company's auditor, director, secretary, senior manager or any other person authorized by the company to receive such disclosures. The protection includes protection from civil and criminal liability (unless the whistleblower also participated in the misconduct) and a prohibition on victimizing the whistleblower.

Although these protections have been in place since 2004, they are often criticized as being ineffective and in need of further reform[2].

Australia also has data protection legislation in place both at the State and Commonwealth level, but this legislation does not directly address whistleblowers or whistleblower information.

2.2 Is an English translation available?

The primary language is English.

[1] Public Interest Disclosure Act 2012 (ACT); Public Interest Disclosures Act 1994 (NSW); Public Interest Disclosure Act 2014 (NT); Public Interest Disclosure Act 2010 (QLD); Whistleblowers Protection Act 1993 (SA); Public Interest Disclosures Act 2002 (TAS); Protected Disclosure Act 2012 (VIC); and Public Interest Disclosure Act 2003 (WA).

[2] See 'Chapter 14: Corporate Whistleblowing: ASIC's Performance and Issues with the Current Protections' of the Senate Standing Committee on Economics' *Final Report on The Performance of the Australian Securities and Investment Commission, June 26, 2014.*

2.3 Is prior notification or approval required?

No. Neither public bodies nor corporations need to notify ASIC or the Office of the Australian Information Commissioner (the data protection regulator) before setting up a whistleblower program[3].

2.4 Can notification or approval be filed online?

Not applicable.

2.5 Generally, how long does it take to get approval?

Not applicable.

2.6 Contact information for Data Protection Authority?

The relevant regulator for corporate whistleblowing is ASIC. ASIC's contact information is as follows:

Firm:	Australian Securities & Investment Commission
Address:	PO BOX 4000 Gippsland Mail Centre VIC 3841, Australia
Telephone:	+61 3 5177 3988 (or if calling from Australia 1300 300 630)
Fax:	+61 3 5177 3999
Email:	feedback@asic.gov.au
Website:	www.asic.gov.au

Alternatively, the contact information for Australia's data protection regulator is as follows:

Firm:	Office of the Australian Information Commissioner
Address:	GPO Box 5218 Sydney NSW 2001, Australia
Telephone:	+61 2 9284 9749 (or if calling from Australia 1300 363 992)
Fax:	+61 2 9284 9666
Email:	enquiries@oaic.gov.au
Website:	www.oaic.gov.au

2.7 What is the scope of reporting permitted?

In order to be protected under the Corporations Act 2001 (Cth), a whistleblower must have reasonable grounds to suspect that a company (or an officer or employee of the company) has or may have contravened a provision of the Corporations Act.

In the public sector, the scope of permissible disclosures varies slightly between jurisdictions but generally covers disclosures of corruption, maladministration and mismanagement of public funds. At the Commonwealth level, the scope of reporting permitted varies depending

[3] See e.g. Whistleblowers Protection Act 2001 Ombudsman's Guidelines accessible at: www.ombudsman.vic.gov.au/getattachment/0021161e-1f8f-4f98-beec-930429752241//publications/guidelines/whistleblowers-protection-act-2001-ombudsman's-gui.aspx

on whether the relevant disclosure is an internal, external, emergency or legal practitioner disclosure, but generally requires a reasonable belief that the information tends to show one or more instances of disclosable conduct.

Under the applicable legislation, "improper conduct" includes corruption, mismanagement of public resources and conduct involving a substantial risk to public health or safety or the environment (if the risk to the environment would constitute a criminal offense).

2.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

Under most State and Territory whistleblower legislation, any natural person can make a public interest disclosure against a public officer or body. This can vary between the states.

Under the Commonwealth legislation, public interest disclosures are only protected if the discloser is, or has been, a public official.

In the private sector, an informant must be a company officer or employee of the company, or a contractor or employee of a contractor, who has a current contract to supply goods or services to the company.

Under the banking and insurance prudential legislation, however, protected disclosures can also be made by persons in a related company. This includes a subsidiary, non-operating holding company, a contractor of an authorized deposit-taking institution, a general insurer, or a person employed by the investment manager or custodian of a superannuation fund trustee. Former employees, financial service providers, voluntary workers and business partners are not afforded protection under the current corporate whistleblower framework.

2.9 Are there limits on who can be a subject of a report?

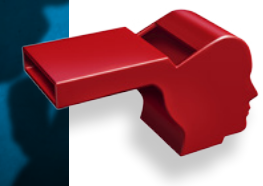
Yes. Under the Corporations Act, a protected disclosure must contain information concerning the company, or an employee or officer of the company.

2.10 Is anonymous reporting permitted?

Generally, anonymous reporting is not permitted in the public or private sector. However, in some State jurisdictions, such as Victoria and Queensland, public interest disclosures can be made anonymously.

2.11 Are there restrictions on the transfer of data in a whistleblowing program?

No, there are no specific provisions that relate to whistleblower information but there is a confidentiality provision in the Corporations Act, which makes it an offense to disclose a protected disclosure, the identity of a whistleblower or information likely to lead to his/her identification that was obtained directly or indirectly from the whistleblower. However, disclosure of any such information to ASIC, the Australian Prudential Regulation Authority ("APRA"), the Australian Federal Police ("AFP") or, if the whistleblower consents, to a third party, is permissible under the Act.



State and Territory whistleblower legislation also contains confidentiality provisions that restrict the transfer of data.

State and Commonwealth data protection legislation provides the same protection to whistleblower information that is personal information and its transfer as it does to any other type of personal information.

2.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No. However, whistleblower consent is required before information contained in a protected disclosure can be disclosed to a third party (other than an authorized entity such as ASIC, APRA or AFP).

2.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

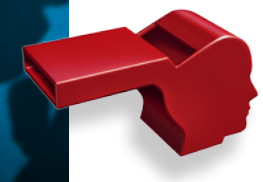
No.

2.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

No.

For more information, contact:

Name:	Veronica Scott or Tarryn Wood
Firm:	Minter Ellison
Address:	Rialto Towers, 525 Collins Street, Melbourne, VIC 3000, Australia
Telephone:	+61 3 8608 2126 or +61 3 8608 2654
Fax:	+61 3 8608 1181 or + 61 3 8608 1000
Email:	veronica.scott@minterellison.com or tarryn.wood@minterellison.com
Website	www.minterellison.com



3. AUSTRIA[4]

3.1 Applicable law and/or data protection guidelines?

Pursuant to Section 99g, para 1 of the Austrian Banking Act, credit institutions and the Austrian Financial Market Authority have to implement whistleblowing programs that allow employees (in the case of the Authority, every person) to notify breaches of bank-related provisions. These programs must comply with the data secrecy principles laid down in the Austrian Data Protection Act 2000 ("the Act").

Otherwise, Austria has no specific whistleblower protection laws in place.

The Austrian data protection authority ("DPA") is the supervisory authority for data protection. The DPA has recently issued decisions relating to the subject (which are not yet available in English).

3.2 Is an English translation available?

For an English version of the Austrian Data Protection Act 2000 see www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.pdf

3.3 Is prior notification or approval required?

Yes. Depending on the scope, the whistleblowing programs have to be either notified or approved. Approval is required when personal data is transferred outside the EU/EEA countries that do not guarantee an adequate level of protection.

3.4 Can notification or approval be filed online?

All data applications have to be notified online (the Act, Section 17, para 1a). Notifications by e-mail or in non-electronic form are admissible for manual filing systems, or in case of a longer-lasting technical blackout of the web application. A guide for the web application can be found on the DPA's website at www.dsb.gv.at/site/7749/default.aspx (but is not yet available in English).

3.5 Generally, how long does it take to get approval?

It usually takes between three to six months to obtain approval from the DPA. Whistleblowing programs involving data relevant under criminal law aspects (including the suspicion of criminal activity), and sensitive data may be started without waiting for approval two months after notification unless the DPA objects to the early start.

[4] Austria is a member state of the European Union. If you are interested in the EU law requirements, please refer to the section on the European Union.

3.6 Contact information for Data Protection Authority?

Name:	Geschäftsstelle der Datenschutzbehörde
Address:	Hohenstaufengasse 3, 1010 Vienna, Austria
Telephone:	+43 1 531 15 / 202525
Fax:	+43 1 531 15 / 202690
Email:	dsb@dsb.gv.at
Website:	www.dsb.gv.at

3.7 What is the scope of reporting permitted?

The DPA has approved the following scope: identification, contact, professional qualification, determination of the circumstances of the case, and data about possible consequent actions. The scope of the report is typically the employee's behaviour at work, but also matters concerning accounting, corruption and financial crimes.

3.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

For compulsory whistleblowing programs under the Austrian Banking Act, see the response to Question 3.1. Regarding voluntary whistleblowing programs, all employees may be entitled to report. It is unclear whether external suppliers may also report under a whistleblowing program.

3.9 Are there limits as to who can be a subject of a report?

The DPA takes a narrower view in line with the Working Paper No. 117 of the Article 29 EC Working Party, and has only approved the transfer of data to non-EEA members under the condition that only management is the subject of a report under the whistleblowing program.

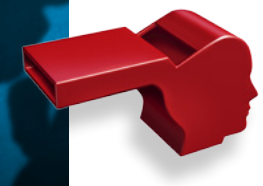
3.10 Is anonymous reporting permitted?

Yes, although anonymous reporting is not encouraged.

3.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes. Data transfer to other EU/EEA countries is not subject to approval but a notification is required. Data transfers outside the EU/EEA countries follow the requirements stated in the Directive 95/46/EC.

Transfer of data to the company's headquarters is only permitted in serious cases.



3.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

It is uncertain whether and under what circumstances the consent of the Works Council (or, in the absence of a Works council, the consent of the employees) is required for the implementation of a whistleblowing program. According to legal literature, consent is required if employees are obliged to report.

3.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

Implementation may require a Works Council's approval (see reponse to Question 3.12).

3.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

The DPA requires a set of conditions to be met.

For more information, contact:

Name:	Robert Keisler or Dr. Bernt Elsner
Firm:	CMS Austria
Address:	Gauermanngasse 2, 1010 Vienna, Austria
Telephone:	+43 1 40443/2850 or +43 1 40443/1850
Fax:	+43 1 40443 9000
Email:	robert.keisler@cms-rrh.com or bernt.elsner@cms-rrh.com
Website:	www.cms-rrh.com

4. BELGIUM[5]

4.1 Applicable law and/or data protection guidelines?

A whistleblower program has to comply with the provisions of the Belgian Act of December 8, 1992 on the protection of privacy in relation to the processing of personal data (hereafter referred to as the "Privacy Act").

Some of the provisions of the Privacy Act are a direct transposition of Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, so that other EU member states should have similar principles.

The Belgian Commission for the Protection of Privacy ("CPP") addressed the specific issue of whistleblowing schemes in its Recommendation 01/2006 of November 29, 2006 regarding the compatibility of whistleblowing with the Privacy Act in relation to the processing of personal data (hereafter the "CPP Recommendation").

The CPP Recommendation provides guidelines as to how the implementation of a whistleblowing scheme can comply with the principles and requirements of the Privacy Act. Some provisions of this Recommendation are inspired by a European text: Opinion 1/2006 provided by the Article 29 Data Protection Working Party on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, anti-bribery, banking and financial crime.

However, please note that the Belgian rules do not limit reporting systems to financial, accounting or auditing matters, provided that the conditions of the Privacy Act are met.

In the public sector, measures have been adopted in 2013 and 2014 to organize a whistleblowing program for employees of the federal administrative authority.

4.2 Is an English translation available?

Yes, see www.privacycommission.be

4.3 Is prior notification or approval required?

Yes, DPA notification is needed.

4.4 Can notification or approval be filed online?

Yes.

4.5 Generally, how long does it take to get approval?

Usually less than three months.

[5] Belgium is a member state of the European Union. If you are interested in the EU law requirements, please refer to the section on the European Union.

4.6 Contact information for Data Protection Authority?

Name:	Belgian Commission for the Protection of Privacy
Address:	139, rue Haute, 1000 Brussels, Belgium
Telephone:	+32 2 213 85 40
Fax:	+32 2 213 85 65
Email:	commission@privacycommission.be
Website:	www.privacycommission.be

4.7 What is the scope of reporting permitted?

No specific limitation is provided for, as long as all conditions of the Privacy Act are met.[6]

According to the CPP Recommendation, there are two grounds upon which the installation of a reporting system can rely:

- A legal or regulatory provision requiring the company to process personal data through such a system, or
- A legitimate interest for the company to install the system, provided that it is not overridden by interests, fundamental rights and freedoms of the concerned data subject.

Please note that a legal obligation in another state, such as the Sarbanes–Oxley Act of 2002, is not considered a valid "legal or regulatory provision (...)" but can constitute a "legitimate interest".

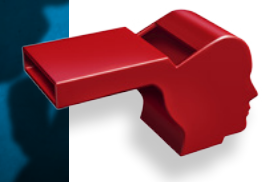
4.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

The CPP Recommendation contains provisions regarding the person/people handling the reports and leading the investigation. The person must:

- Be specially dedicated to this function;
- Hold to professional confidentiality;

[6] Article 5 of the Privacy Act provides that personal data can only be processed in the following limited cases:

a) The data subject has unambiguously given his/her consent;
b) The processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
c) The processing is necessary for compliance with an obligation to which the controller is subject to, or by virtue of an act, decree or ordinance;
d) The processing is necessary in order to protect the vital interests of the data subject;
e) The processing is necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller or in a third party to whom the data is disclosed;
f) If the processing is necessary for the safeguard of the legitimate interests of the controller or the third party to whom the data is disclosed, except where such interests are over-ridden by the interests or fundamental rights and freedoms of the data subject claiming protection under this Act.



- Be able to act with sufficient independence;
- Be subject to liability in case of breach of the confidentiality; and
- Be protected from pressure from his/her hierarchy or professional organizations.

The whistleblower must also be protected from the consequence of a fault of the person handling the reports.

In addition, the entities handling the reports must assure that:

- The personal data be adequate, pertinent and not excessive;
- The data are limited to factual description without value judgement;
- It is explicitly indicated where the facts are unproven; and
- The data are not conserved more than the time necessary for its processing (though no specific time limitation is mentioned (contrary to France).

In case an external service provider undertakes the handling of the reports, the company is responsible for this entity so that it must ensure that the outsourcing service complies with the aforementioned requirements.

4.9 Are there limits as to who can be subject of a report?

No.

4.10 Is anonymous reporting permitted?

Anonymous reports are in principle forbidden but the CPP Recommendation states that it refers to the EU Opinion of the Article 29 Working Party regarding this question. Accordingly, there must be promotion of identified and confidential reports versus anonymous reports.

Anonymous reports are exceptionally allowed in so far as:

- Anonymity is not mandatory;
- Anonymity is not encouraged as the usual way to make a complaint;
- The company does not advertise the fact that anonymous reports may be made through the scheme; and
- The scheme informs the whistleblower that his/her identity will be kept confidential at all the stages of the process.

4.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes. If the personal data are transferred to a third country outside the European Union, the data controller shall assure that the country is provided with an adequate level of protection and that it complies with the provisions of the Privacy Act.

The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations. Particular consideration should be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and the country of final destination, the rules of law, both general and sectoral, in force in the third country in question, and the professional rules and security measures that are complied with in that country.

Please note again that the Belgian rules regarding transfer of the data to third countries are a very close transposition of the EU data protection directive cited above.

4.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

The answer to this question will depend on the concrete elements of the whistleblowing program that the company wants to put in place.

4.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

Yes. When introducing a whistleblowing program, the employer will need to inform the workers collectively (through the Works Council, the Prevention and Protection Committee or the unions) as well as individually. In an ideal situation, the employer obtains the worker's consent, e.g., by making him/her sign a copy of the policy for approval.

4.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

Yes. The reporting scheme must have safeguards so that the data cannot be unlawfully deleted, cannot be processed for other purposes than those defined, etc. These should be described in the policy.

For more information, contact:

Name: Renaud Dupont
Firm: CMS Belgium
Address: Chaussee de La Hulpe 178, B-1170 Brussels, Belgium
Telephone: +32 2 743 69 83
Fax: +32 2 743 69 01
Email: renaud.dupont@cms-db.com
Website www.cms-db.com

5. BRAZIL

5.1 Applicable law and/or data protection guidelines?

Brazil has no specific whistleblower protection laws in place. However, there are various pieces of legislation and jurisprudence that provide certain guidelines, although they do not directly address the issue.

Moreover, the Brazilian Federal Constitution of 1988 grants protection to and the privacy of any Brazilian citizen's personal data and, further, the inviolability of any Brazilian citizen's intimacy and personal life. Any Brazilian citizen who has these constitutional rights violated is entitled to claim for moral damages. Therefore, when conducting internal investigations based on allegations reported through the whistleblowing program, companies should take certain precautions to ensure that only the personnel involved in the investigation have access to the information, that security measures are adopted to ensure that the information is not disclosed to third parties, and that the information is only used for the purpose of the internal investigation, so as to avoid claims for moral damages.

It is also worth noting, at this point, that data involved in a whistleblowing program is not deemed personal data for Brazilian law purposes, to the extent that communications in a whistleblowing program involves corporate e-mails, documents and other items that constitute property of the employer, and not of the employee.

5.2 Is an English translation available?

Not applicable.

5.3 Is prior notification or approval required?

There is no data protection authority in Brazil and no prior notification or approval is required.

5.4 Can notification or approval be filed online?

Not applicable.

5.5 Generally, how long does it take to get approval?

Not applicable.

5.6 Contact information for Data Protection Authority?

Not applicable.

5.7 What is the scope of reporting permitted?

From a Brazilian law perspective, there are no limits to the scope of reporting permitted.

5.8 Are there limits as to who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No, from a Brazilian law perspective, the whistleblowing program may be accessible for reporting to any type of employee as well as to third parties, such as contractors, vendors, agents and/or other stakeholders.

5.9 Are there limits as to who can be a subject of a report?

No, there are no limits as to who can be the subject of a report.

5.10 Is anonymous reporting permitted?

Yes, the whistleblowing program may be set up to allow anonymous reporting.

5.11 Are there restrictions on the transfer of data in a whistleblowing program?

Brazilian law does not prohibit or restrict the transfer of data in a whistleblowing program, even if such transfer is made to other countries.

5.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No, from a Brazilian law perspective, no consent of employees is required for a whistleblower program or for the transfer of data in a whistleblowing program.

5.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

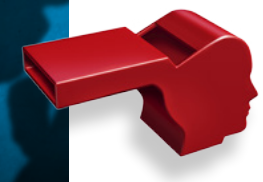
No, from a Brazilian law perspective, no consent or consultation with a Works Council, union or other employee representative group is required.

5.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

No, there are no specific computer or other security requirements for the whistleblower program.

For more information, contact:

Name: Renata Muzzi Gomes de Almeida
Firm: TozziniFreire Advogados
Address: Rua Borges Lagoa, 1328, Sao Paulo, SP, 04038-904, Brazil
Telephone: +55 11 5086 5000
Fax: +55 11 5086 5555
Email: rmuzzi@tozzinifreire.com.br
Website www.tozzinifreire.com.br



6. BULGARIA[7]

6.1 Applicable law and/or data protection guidelines?

No, Bulgaria has no specific whistleblower protection laws in place. The issue of whistleblowing occurs in a number of different statutes such as the Administrative Procedure Code, the Labour Code, the Civil Servants Code, the Criminal Code, and the Data Protection Law. However, they mostly apply to the public sector and address the issue quite generally and indirectly.

6.2 Is an English translation available?

Yes. There are official English translations of the relevant statutes.

6.3 Is prior notification or approval required?

No, it is not necessary to notify the Data Protection Authority ("DPA") or seek approval from any agency or authority to set up a whistleblower program. However, a whistleblower program has to comply with data protection rules as long as a company collects and processes personal data through its whistleblower system.

6.4 Can notification or approval be filed online?

Not applicable.

6.5 Generally, how long does it take to get approval?

Not applicable.

6.6 Contact information for Data Protection Authority?

Name:	Commission for Personal Data Protection
Address:	2 Prof. Tsvetan Lazarov Blvd., 1592 Sofia, Bulgaria
Telephone:	+359 2 9153 518
Email:	kzld@cpdp.bg
Website:	www.cpdp.bg

6.7 What is the scope of reporting permitted?

There is no strictly defined legal scope of reporting. The different statutes applicable to whistleblowing contain non-exhaustive enumerations of various wrongdoings that could be subject to reporting. For instance, the Bulgarian Administrative Procedure Code stipulates that reports could be filed for abuse of power and corruption, mismanagement of state or municipal property, or other irregularities and omissions of administrative bodies and public officials. The wrongdoings should be of such nature as to affect state or public interests, or the rights or legitimate interests of other persons.

[7] Bulgaria is a member state of the European Union. If you are interested in the EU law requirements, please refer to the section on the European Union.

6.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No. The Bulgarian Administrative Procedure Code stipulates that every natural or legal person (citizens and organizations), as well as the ombudsman, can report suspicions of corruption.

6.9 Are there limits on who can be a subject of a report?

No.

6.10 Is anonymous reporting permitted?

Certain restrictions on anonymous reporting apply, especially in the public sector. The Bulgarian Administrative Procedure Code stipulates that anonymous reports will be given no consideration.

6.11 Are there restrictions on the transfer of data in a whistleblowing program?

General data protection rules apply. Data transfer to other EU/EEA countries is not subject to approval by the Bulgarian DPA. Data transfers outside the EU/EEA countries follow the requirements stipulated in the Directive 95/46/EC.

6.12 Is the consent of employees required either for a whistleblower program or for the transfer of data in a whistleblowing program?

If the program involves the use of personal data, the employee's prior consent could be required as an alternative precondition for the data processing in line with the Directive 95/46/EC.

6.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

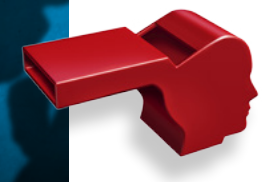
No.

6.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

General data protection rules apply. In light of Directive 95/46/EC, the personal data administrator must implement appropriate technical and organizational measures to protect the data against accidental or unlawful destruction, or against accidental loss, unauthorized access, alteration or dissemination, and against other unlawful forms of data processing.

For more information, contact:

Name: Desislava Todorova
Firm: CMS Bulgaria
Address: 4 Knyaz Alexander I Battenberg Str., fl. 2, 1000 Sofia, Bulgaria
Telephone: +359 2 447 1321
Fax: +359 2 447 1390
Email: desislava.todorova@cms-rrh.com
Website: www.cms-rrh.com



7. CANADA

7.1 Applicable law and/or data protection guidelines?

Neither the Canadian government nor the provinces of Quebec or Ontario have enacted special legislation regulating the creation of "whistleblowing programs". However, a number of provincial and federal laws contain provisions that shield employees who inform designated government or company officials about offenses or contraventions of the law in question from their employer's potential reprisal.

For example, the Public Servants Disclosure Protection Act, SC 2005, c. 46 establishes a procedure for the disclosure of wrongdoings in the federal public sector, including the protection of persons who disclose the wrongdoings.

For another example, the Personal Information Protection and Electronic Documents Act SC 2000, c. 5 ("PIPEDA"), which is designed to protect the collection, disclosure, or use of personal information, protects the anonymity of individuals who inform the Privacy Commissioner of Canada of breaches of the rules pertaining to the protection of personal information.

For a final example, the Ontario Securities Commission has also adopted National Instrument 52-110, which provides that every issuer of securities must establish an Audit Committee to fulfill the requirements established by that directive. Section 2.3 (7) provides that the Audit Committee must establish procedures for the confidential, anonymous submission of concerns regarding questionable accounting or auditing matters by employees of the issuer.

7.2 Is an English translation available?

Yes, for Canada's Personal Information Protection and Electronic Documents Act, see: www.canlii.org/en/ca/laws/stat/sc-2000-c-5/latest/sc-2000-c-5.html.

7.3 Is prior notification or approval required?

National Instrument 52-110 requires that an issuer's Audit Committee establish what may be termed a "whistleblower program" over questionable accounting or auditing practices. This National Instrument does not expressly require that the Audit Committee have its program approved by a public authority.

7.4 Can notification or approval be filed online?

Not applicable.

7.5 Generally, how long does it take to get approval?

Not applicable.

7.6 Contact information for Data Protection Authority?

There is no organization or individual in Canada that has been explicitly appointed as Canada's data protection authority. However, the Privacy Commissioner is an advocate for the privacy rights of Canadians. The Privacy Commissioner's powers include:

- Investigating complaints, conducting audits and pursuing court actions under certain federal laws;
- Publicly reporting on the personal information-handling practices of public and private sector organizations;
- Supporting, undertaking and publishing research into privacy issues; and
- Promoting awareness and understanding of privacy issues.

In addition, individuals can complain to the Commissioner about certain matters, and the Commissioner may also investigate complaints regarding private-sector bodies. There are also agencies in each of the provinces that deal with information and privacy issues.

Name:	Office of the Privacy Commissioner of Canada
Address:	30 Victoria Street, Gatineau, Quebec K1A 1H3, Canada
Telephone:	+1 819-994-5444 or +1 800 282 1376
Email:	via online request form: https://www.priv.gc.ca/cu-cn/index_e.asp
Website:	www.priv.gc.ca

7.7 What is the scope of reporting permitted?

Generally speaking, legislative provisions that shield "whistleblowers" from reprisal are contained in broader statutes. As a result, an employee will be shielded from reprisals for reporting when the employee has reported an offense under the Act in question. For example, the Ontario Securities Commission's National Instrument 52-110 provides that an Issuer's Auditing Committee must establish procedures to solicit employee complaints on "questionable accounting or auditing matters".

7.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

The aforementioned statutes will either be limited to employees or to workers or will be extended to all persons.

PIPEDA provides protection for any person. PIPEDA also explicitly provides protection to employees against their employers. An "employee" includes an independent contractor in this context.

7.9 Are there limits as to who can be a subject of a report?

Legislation enacted by the Canadian Parliament and the provincial legislatures are typically silent on this issue. However, the Criminal Code restricts protection to employees who have disclosed a potential offense committed by the employer, an officer or employee of the employer or, if the employer is a corporation, by one or more of its directors. Anyone can be reported to the Commissioner under PIPEDA.

7.10 Is anonymous reporting permitted?

National Instrument 52-110 requires that an Auditing Committee establish procedures for the "confidential, anonymous submission by employees of the issuer." Thus, each Auditing Committee must establish a procedure that guarantees that submissions remain confidential and anonymous. The Instrument is silent as to how this may reasonably be accomplished.

PIPEDA provides that the Commissioner shall keep confidential the identity of a person who has notified the Commissioner of a breach of the provisions set out in PIPEDA regarding the protection of personal information, provided that the Commissioner has given that person an assurance of confidentiality.

7.11 Are there restrictions on the transfer of data in a whistleblowing program?

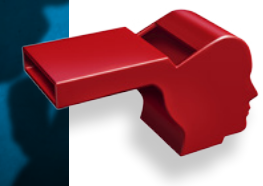
Regarding privacy laws in Canada, the provinces of Québec, British Columbia, Alberta and Manitoba are the only jurisdictions to have enacted comprehensive privacy laws applicable to the private sector. PIPEDA applies to provinces that have not yet enacted similar legislation (s. 26 (2) b) PIPEDA).

Under PIPEDA, the transfer of an individual's personal information across borders requires that the organization that is in control of the personal information notify the individual whose personal information is to be transferred, and, in the case of transfers of personal information to the U.S., warn them about that country's Patriot Act.

In Canada, privacy laws are based on the premise that an individual has the right to have access to information collected on him/her. Therefore, the protection of whistleblowers' personal information is structured in the form of restrictions or prohibitions on communicating the information under certain circumstances.

Under Section 9 of PIPEDA, an organization cannot give an individual access to personal information if doing so would likely reveal personal information about a third party. An organization is not required to give access to personal information if, among other things:

1) Doing so could reasonably be expected to threaten the life or security of another individual;



2) The information was created for the purpose of making a disclosure under the Public Servants Disclosure Protection Act or in the course of an investigation into a disclosure under that Act; or

3) The information collected related to investigating a breach of an agreement or a contravention of a federal or provincial law.

In Québec, Section 39 of the Act Respecting the Protection of Personal Information in the Private Sector, R.S.Q., c. P-39.1, provides that an organization can refuse to communicate personal information to the person it concerns where disclosure of the information would be likely to hinder an inquiry, the purpose of which is the prevention, detection or repression of crime or statutory offenses conducted by an internal security service or conducted on behalf of an external service. Section 40 provides that an organization must refuse to provide personal information to a person to whom it relates where disclosure would be likely to reveal personal information about a third person, or the existence of such information and its disclosure may seriously harm that third person.

The privacy laws of the provinces of British Columbia, Alberta and Manitoba have similar protections.

7.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

There exists no such express formal requirement. As discussed above, under PIPEDA, the transfer of an individual's personal information across borders will require that the organization that is in control of the personal information notify the individual whose personal information is to be transferred, and, in the case of transfers of personal information to the U.S., warn them about the U.S. Patriot Act.

7.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

No.

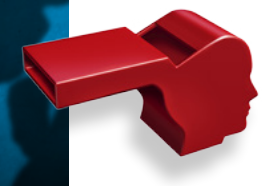
7.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

There are no specific provisions pertaining to computer or security requirements regarding information collected from a whistleblower set out in PIPEDA or in any other Canadian statute or regulation discussed above.

For more information, contact:

Name: Stéphane Eljarrat
Firm: Davies Ward Phillips & Vineberg LLP
Address: 1501 McGill College Avenue, 26th Floor, Montréal QC H3A 3N9, Canada
Telephone: +514 841 6439
Fax: +514 841 6499
Email: seljarrat@dwpv.com
Website: www.dwpv.com

Name: Peter Ruby
Firm: Goodmans LLP
Address: Bay Adelaide Centre, 333 Bay Street, Suite 3400, Toronto, ON, M5H 2S7, Canada
Telephone: +416 597 4184
Fax: +416 979 1234
Email: pruby@goodmans.ca
Website: www.goodmans.ca



8. CHILE

8.1 Applicable law and/or data protection guidelines?

Chile has no specific whistleblower protection laws in place. However, the processing and/or use of information obtained within whistleblower programs shall not be in conflict with the Data Protection Act or the Labour Code.

8.2 Is an English translation available?

No.

8.3 Is prior notification or approval required?

No.

8.4 Can notification or approval be filed online?

Not applicable.

8.5 Generally, how long does it take to get approval?

Not applicable.

8.6 Contact information for Data Protection Authority?

There is currently no Data Protection Authority in Chile.

8.7 What is the scope of reporting permitted?

There is no specific legislation but the processing and/or use of information obtained within whistleblower programs shall not be in conflict with the Data Protection Act, nor breach certain worker rights established in the Labour Code.

8.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

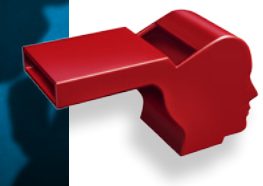
Not applicable.

8.9 Are there limits as to who can be a subject of a report?

Not applicable.

8.10 Is anonymous reporting permitted?

Yes.



8.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes. As a general rule, the processing or use of personal information, whether within a whistleblower program or not, must be authorized by law or approved in writing by the owner of the data. The person that gives his/her consent should be duly informed about the storage and purpose of his/her personal data and its potential disclosure to the public. In specific cases established under the Data Protection Act, such as the processing of personal data that comes or is collected from public sources and has an economic, financial, banking or commercial character, no consent is required.

In addition, no approval is required if private legal entities handle personal data for their exclusive use, or use by their associates and by the entities to which they are affiliated, as far as it is used for statistical or pricing purposes, or for any general benefit of those indicated above. However, sensitive information may only be transferred or used if authorization is granted by a specific law or by the owner of the data, or if such data is necessary for granting health benefits to the holder of the information.

On the other hand, the processing and/or use of information obtained within a whistleblower program shall not breach certain worker rights. For instance, Art. 154 *bis* of the Labour Code provides that the employer shall maintain confidentiality of all private information and data regarding employees obtained during the employment relationship.

8.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

Yes. If no authorization is granted by law, the transfer of personal or sensitive data of an employee within a whistleblowing program requires his/her written consent.

8.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

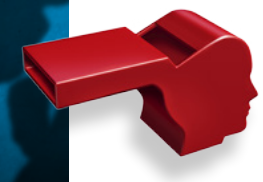
No.

8.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

No.

For more information, contact:

Name: Sergio Orrego or Nicholas Mocarquer
Firm: Urenda, Rencoret, Orrego y Dörr
Address: Av. Andrés Bello 2711, 16th floor, 7550611 Las Condes, Santiago - Chile
Telephone: +562 2499 5531
Fax: +562 2499 5555
Email: sorrego@urod.cl or nmocarquer@urod.cl
Website: www.urod.cl



9. CHINA, PEOPLE'S REPUBLIC OF

9.1 Applicable law and/or data protection guidelines?

In mainland China, reporting wrongdoings of public officers to public authorities is highly encouraged and is stipulated as a fundamental right in Article 41 of the Constitution of China. Furthermore, according to Article 108 of the Criminal Procedure Law of China, any person has the right and duty to report relevant information to public authorities upon discovering a crime conducted by any other person or entity. If any whistleblowing program run by the company hinders its employees from reporting wrongdoings, certain fines may be imposed on the company.

There is no specific whistleblower protection law in place. Instead, a number of whistleblowing-related provisions are found in various legislation and, to some extent, play essential roles in encouraging and protecting disclosures of wrongdoings. In China, whoever retaliates against whistleblowers shall be punished with administrative sanctions or charged with certain crimes if the circumstances are serious.

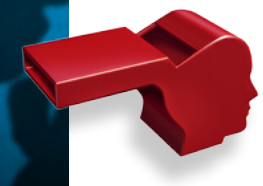
For example, the "Rules of the Supreme People's Procuratorate on Protecting the Citizens' Tip-off Rights" promulgated on May 13, 1991, clearly provides that "procuratorial organizations shall keep strictly secret the relative information of the crime reporter, such as name, employing unit and family dwelling place and the impeaching contents, and shall not extract and copy the tipping documents without authorization." (The Supreme People's Procuratorate is the highest agency at the national level responsible for both prosecution and investigation in the People's Republic of China.)

Provisions of the People's Procuratorate on "Reporting of Crimes" also provide legal protections to whistleblowers who have reported criminal acts (e.g., corruption, bribery, malfeasance), under which it is strictly prohibited to disclose the content of reported information or the personal information of the whistleblower to the person or entity being reported against.

China's "Tort Liability Law" and "Consumer Rights Protection Law" respectively, which took effect on July 1, 2010 and January 1, 1994 (amended March 15, 2014), also contain provisions for the protection of individual privacy, according to which the processing and/or use of information obtained within a whistleblowing program shall not breach the privacy rights of both the whistleblower and the person or entity being reported against.

If state-secret issues appear during the operation of a whistleblowing program, mostly in the case of a joint venture enterprise to which a state-owned enterprise is a party, the "Law of China on Guarding State Secrets" shall apply, and references to a state secret shall be limited to the minimum required for the whistleblowing report.

In addition, most public authorities have released detailed regulations within their respective administrative areas to facilitate the disclosure of unlawful behaviours in connection with



accounting, internal accounting controls, auditing matters, corruption, bribery, safety production, taxation, the labour system, environmental violations, etc. In general, reporting rewards and protection measures are provided correspondingly.

9.2 Is an English translation available?

English translations for some of the above-mentioned laws are available on the government's official websites.

Constitution of China:
www.npc.gov.cn/englishnpc/Law/2007-12/05/content_1381903.htm

Criminal Procedure Law of China:
www.npc.gov.cn/englishnpc/Law/2007-12/13/content_1384067.htm

Provisions of the People's Procuratorates on Reporting of Crimes:
www.lawinfochina.com/display.aspx?id=7651&lib=law

Tort Liability Law of China:
http://english.taizhou.gov.cn/art/2013/8/22/art_1590_249830.html

Law of China on Guarding State Secrets:
www.npc.gov.cn/englishnpc/Law/2007-12/12/content_1383925.htm

Some third-party providers, such as Westlaw and Bei Da Fa Bao, may also provide English translations for laws and regulations for reference, but membership may be required for access.

9.3 Is prior notification or approval required?

No. A company does not need to notify any public authority before setting up a whistleblowing program.

9.4 Can notification or approval be filed online?

Not applicable.

9.5 Generally, how long does it take to get approval?

Not applicable.

9.6 Contact information for Data Protection Authority?

In a general sense, there is no single public authority that supervises protection of personal information. However, regarding the personal information of telecommunications and internet users, the Ministry of Industry and Information Technology and other relevant entities are the supervisory authorities.

Name: Ministry of Industry and Information Technology
Address: Chang'an Avenue 13, Beijing, China, 100804
Telephone: +86 10 68205985; +86 10 66012374
Website: www.miit.gov.cn

As to the personal information relating to commerce and business, the Administration for Industry and Commerce ("AIC") is the supervisory authority.

Name: Administration for Industry and Commerce
Address: East San He Li Road 8, Xicheng District, Beijing, China, 100820
Telephone: +86 10 88650000
Email: dfa@saic.gov.cn
Website: www.saic.gov.cn

9.7 What is the scope of reporting permitted?

There is no legal restriction on the scope of reporting permitted. Generally, all activities in violation of various laws and regulations could be reported, while fabrication or distortion of facts for purposes of libel or false incrimination are prohibited. However, each public authority may only accept or deal with certain types of reports falling into its own judicial or administrative authority.

In addition, activities contrary to the internal policies of a company could be reported to the company's internal compliance section, its management (e.g., a supervisor) or the competent government department (e.g., AIC).

9.8 Are there limits as to who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No, there is no such legal restriction. Restricting employees' right to report suspected criminal acts may trigger administrative sanctions or criminal punishments against the company.

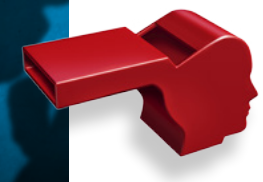
In addition, in China even a criminal or suspect himself/herself has a right to report another person's illegal activities.

9.9 Are there limits as to who can be a subject of a report?

No, there is no such limit.

9.10 Is anonymous reporting permitted?

Yes, anonymous reporting is permitted. However, real-name reporting will usually obtain more attention both from public authorities and private companies. Some laws and regulations also provide that official responses must be made to real-name reporters within a certain time limit. In addition, in some cases, awards arising from effective whistleblowing are granted only to real-name whistleblowers. Note, however, that in related litigation, if state secrets or trade secrets or personal privacy are involved, the court or the concerned party may require a hearing in a non-public session.



9.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes. If the data transferred involves employees' privacy or a trade secret, the consent of such employee or the owner of the trade secret is needed. If the transferred data is categorized as a state secret, numerous special rules apply relating to data storage, data transmission, access restrictions to such data, etc.

9.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No. However, if a whistleblowing program includes provisions related to employees' vital interests, the company shall consult with and obtain the approval of the labour union or employees' representatives. Where a data transfer in a whistleblowing program involves personal information that bears on an employee's privacy, the consent of the employee must be obtained.

9.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

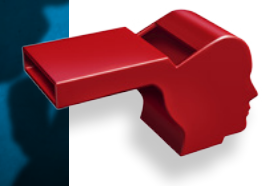
No. See the response to Question 9.12.

9.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

Yes. For reports to public authorities, detailed requirements have been stipulated with respect to the preservation of reported information. For instance, reported information received by the People's Procuratorate shall be recorded in a dedicated computer by specially assigned staff and only authorized persons may have access to such information.

For more information, contact:

Name: Gary Gao
Firm: Zhong Lun Law Firm
Address: Level 10 & 11, Two IFC, No. 8 Century Avenue, Pudong New Area, Shanghai 200120, PRC
Telephone: +86 21 60613666
Fax: +86 21 60613555
Email: gaojun@zhonglun.com
Website: www.zhonglun.com



10. COLOMBIA

10.1 Applicable law and/or data protection guidelines?

No, Colombia has no specific whistleblower protection laws in place. However, a number of laws contain provisions that would be applicable to whistleblowing programs. For instance, Law 1010 of 2006 regulates labour harassment. This law defines, prevents and sanctions labour harassment behaviours by implementing certain rights and remedies in order to prevent any retaliation against employees who have claimed or disclosed labour harassment. Likewise, whistleblowing programs must also comply with the provisions of Law 1581 of 2012, the Colombian general personal data protection law (DPL).

10.2 Is an English translation available?

No.

10.3 Is prior notification or approval required?

No, it is not necessary to notify or request authorization from the Data Protection Authority ("DPA") to set up a whistleblower program.

10.4 Can notification or approval be filed online?

Not applicable.

10.5 Generally, how long does it take to get approval?

Not applicable.

10.6 Contact information for Data Protection Authority?

Name:	Deputy Superintendent of Personal Data Protection
Address:	German Enrique Bacca Medina
Telephone:	+571 58 70247 Ext: 70001
Email:	habeasdata@sic.gov.co
Website:	www.sic.gov.co

10.7 What is the scope of reporting permitted?

There are no limitations to the scope of reporting permitted in whistleblowing programs in Colombia, provided that such programs do not conflict with the above-mentioned general labour harassment laws or personal data protection laws. Thus, whistleblowing programs cannot go beyond the scope of employment, and information processed thereunder cannot exceed the scope of the authorization provided by the data owner.

10.8 Are there limits as to who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No.

10.9 Are there limits as to who can be a subject of a report?

No.

10.10 Is anonymous reporting permitted?

Yes. Anonymous reporting is permitted. However, the company must afford employees the full right of defense.

10.11 Are there restrictions on the transfer of data in a whistleblowing program?

According to the DPL, international transfers of personal data are prohibited unless the country where the data will be processed provides adequate levels of data protection. This prohibition will not apply when:

- The country where the data will be processed affords adequate protection of personal data;
- The data owner has expressly authorized the cross-border transfer of data;
- There is an exchange of medical data;
- The transfer relates to bank and stock transfers;
- The transfer takes place as agreed under international treaties to which Colombia is a party;
- The transfer is necessary for the execution of a contract between the data owner and the controller, or for the implementation of pre-contractual measures, provided there is consent of the data owner; or
- The transfer is legally required to safeguard the public interests of the country.

Furthermore, transmission of personal data (i.e., a transfer from a controller to a processor) requires that: (a) the controller has obtained express authorization from the data owner in order to transmit the information to the processor; or (b) the controller and the processor have entered into a data-processing agreement.

10.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No specific requirements exist concerning employees' consent for whistleblower programs, other than general authorization requirements for processing of personal data under personal

data protection laws. The consent of employees for transfer of data is required on the terms explained above, in response to Question 10.11.

10.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

No, provided that the collective labour agreement with the union or any other company policy do not stipulate otherwise.

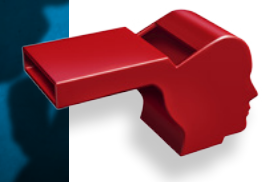
10.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

There are no specific computer or other security requirements concerning whistleblower programs. However, as a general rule, personal data can only be retained for as long as it is reasonable and necessary and in accordance with the purposes of the processing authorized by the data owner. Also, the controller must implement all due measures to guarantee the security and confidentiality of personal data.

Under Colombia's labour regulations, there is a three-year statute of limitations, requiring employers to keep information accordingly.

For more information, contact:

Name: Diego Cardona
Firm: Philippi, Prietocarrizosa &Uría
Address: Carrera 9 # 74-08, Bogota D.C., Colombia
Telephone: +571 326 8600 Ext. 1419
Fax: +571 326 8419
Email diego.cardona@ppulegal.com
Website: en.ppulegal.com



11. COSTA RICA

11.1 Applicable law and/or data protection guidelines?

Costa Rica does not have a specific whistleblower protection law in place.

However, since whistleblowing programs rely in the vast majority of cases on the processing of personal data, the rules and principles of the Law on Individual Protection for Processing of Personal Data (the "Data Protection Law") and its Regulations, which became effective on March 6, 2013, could apply to whistleblowing programs. Additionally, case law of the Constitutional Court, Law on Individual Protection for Processing of Personal Data, Nº 8968 dated July 7, 2011, and Article 196 of the Costa Rican Criminal Code, contain the main data protection provisions.

On the other hand, it is important to mention that the Criminal Procedural Code (Law No. 7596), the Law Against Government Corruption and Illicit Enrichment (Law No. 8422) and the Law of Private Security Services (Law. No. 8395) list specific persons who are required to complete a mandatory criminal claim filing if they are aware of a public offense related to corruption or mismanagement of private funds.

Finally, the Law for Protection of Victims, Witnesses and Other Judicial Parties (from October 4, 2006) protects the rights and interests of these people within a judicial proceeding if there is an actual danger to them or with respect to their current, future or eventual participation during a criminal proceeding. The protection may also be extended to their relatives.

11.2 Is an English translation available?

Contact the author for a translation.

11.3 Is prior notification or approval required?

There are no specific conditions for prior approval of a whistleblower program. However, the data privacy law includes certain provisions when sharing personal data, which will require prior notification to the Data Protection Agency, known as "PRODHAB".

In this case, if the database includes sensitive or restricted information, or if the whistleblower program database will be transferred outside the country, or if its contents will be sold, distributed or shared with a third party, then the database should be registered with PRODHAB. In other words, if the implementation of the whistleblower program involves any of these elements, it will be mandatory to register the program as a database.

11.4 Can notification or approval be filed online?

No, there is no online notification filing.

In the event that there are databases subject to filing requirements, these databases must be registered with PRODHAB with the following information:

- Names of the databases;
- Types of personal data held in the databases;
- Purpose and foreseen uses of the databases;
- Indication of the party responsible for the databases before PRODHAB and before third parties;
- Identification of technology intermediaries and the contract that governs their relationship (required by Article 30 of the Regulation);
- Security measures for protecting the databases;
- Minimum protocols applicable to the databases;
- Informed consent form;
- A "super user" account to access the databases (PRODHAB requires a sworn declaration that access will be allowed in the case of any claim of data breach);
- International contracts and information regarding the sale of any data bases; and
- Proof of training of personnel.

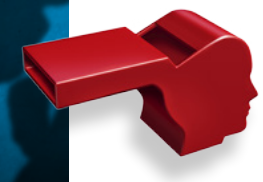
Once all the forms and functional requirements are fulfilled by the applicant, an annual fee of USD 200 must be paid to PRODHAB to finalize the registration of the databases.

11.5 Generally, how long does it take to get approval?

If all the information is dully completed, PRODHAB will register the database within one month.

11.6 Contact information for Data Protection Authority?

Name:	Agencia de protección de datos de los habitants (PRODHAB)
Address:	Edificio Administrativo del Registro Nacional (Módulo 8) 4° piso
Telephone:	+506 2528 33 15
Email:	protecciondedatos@mj.go.cr
Website:	www.prodhab.go.cr



11.7 What is the scope of reporting permitted?

As mentioned above, Costa Rica has no specific whistleblower protection laws in place. Therefore, there are no particular limits to the scope of reporting permitted, except for certain parameters set by the labour laws, constitutional rights, and data privacy laws, which a company setting up a whistleblowing program must follow.

Also, as mentioned above, any database created through the whistleblowing program needs to be registered with PRODHAB.

In addition, a company implementing a whistleblowing program must include a non-retaliation provision and ensure confidentiality of the process to protect employees´ dignity and privacy at all times. Also, it is recommended that the scope of reporting must not include facts beyond the scope of employment or relationship with the company.

As a best practice, a privacy reminder should be added to the whistleblowing program.

11.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

There is no specific requirement in the law.

11.9 Are there limits on who can be subject of a report?

No, there is no specific requirement in the law.

11.10 Is anonymous reporting permitted?

Yes, anonymous reporting is permitted.

11.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes. According to the data privacy law, all personal data that is transferred to a third party inside or outside the country most comply with the PRODHAB registration requirements.

11.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

Yes, informed consent is required for such purposes.

11.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

No, this is not required by the law.

11.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

The Responsible Party must keep a register of security incidents. In addition, the law requires that security measures must be stablished if a data breach incident occurs. If a data breach incident occurs, the Responsible Party must notify PRODHAB and the data owner.

The Law makes a distinction between a party responsible for a database (the "Responsible Party") and a party handling a database (hereinafter, the "Handling Party") which is illustrated by the definitions in the Law provided below:

"The party responsible for the database is a physical or legal person *that administers, manages or is in charge of the database*, whether this is a public or private entity, which is competent under the law to *decide the purpose of the database, what categories of personal information will be registered in it and what type of treatment will be applied to it.*"[8] (Emphasis not in original).

"Party Handling Databases: All physical and legal persons, whether public or private, or any other entity *that handles personal data for the account of the party responsible for the database*".[9] (Emphasis not in original).

The Responsible Party will determine the security measures applicable to the personal data handled or stored, considering the following factors:

- The sensitivity of the personal data handled, as permitted by law;
- The state of technology development;
- The possible consequences of a breach for the owners of the personal data;
- The number of owners of personal data;
- The breaches that have previously occurred in the handling and storage systems being used;
- The risk presented to the personal data based on their quantitative or qualitative value; and
- Other factors that arise under other laws or regulations applicable to the Responsible Party.

For more information, contact

Name: Valeria Agüero or Carolina Muñoz
Firm: Arias & Muñoz
Address: Costa Rica, Centro Empresarial Forum 1, Edificio C, oficina 1C1.
Telephone: +506 2503 9800
Fax: +506 2204 7580
Email: vaguero@ariaslaw.co.cr or cmunoz@ariaslaw.co.cr
Website: www.ariaslaw.com

[8] Article 3 of the *Law on Individual Protection for Processing of Personal Data.*
[9] Article 2 of the *Regulation to the Law on Individual Protection for Processing of Personal Data.*

12. CROATIA[10]

12.1 Applicable law and/or data protection guidelines?

Croatia has no specific whistleblower protection laws in place. However, there are labour laws, data protection laws ("DPL") and other regulations (the Penal Code, the Labour Act, the Trade Act, the Civil Servants Act, the Act on Protection of Data Confidentiality) which provide certain guidelines, particularly regarding the protection from discrimination of employees and civil servants who report corruption and other irregularities. However, apart from general provisions on protection of whistleblowers, these laws do not explicitly regulate the matter.

The Croatian Data Protection Agency ("DPA") is the supervisory authority for data protection.

12.2 Is an English translation available?

An unofficial translation of the Personal Data Protection Act is available at: www.azop.hr/page.aspx?PageID=79.

12.3 Is prior notification or approval required?

No, it is not required by law to notify the DPA or seek approval from any agency or authority to set up a whistleblower program.

Nevertheless, as the whistleblower program may include creation of a database with personal data of the employees, a company must generally comply with the requirements in accordance with the DPL, including the notification of a personal database.

12.4 Can notification or approval be filed online?

Yes, notification of a personal database can be filed online with the Central Register of the DPA.

12.5 Generally, how long does it take to get approval?

Not applicable as there is no approval process in place. Only notification of the database is required.

12.6 Contact information for Data Protection Authority?

Name:	Data Protection Agency (Croatian: "Agencija za zaštitu osobnih podataka")
Address:	Martićeva 14, 10 000 Zagreb, Croatia
Telephone:	+385 1 4609-000
Fax:	+385 1 4609-099
E-mail:	azop@azop.hr
Website:	www.azop.hr

[10] Croatia is a member state of the European Union. If you are interested in the EU law requirements, please refer to the section on the European Union.

12.7 What is the scope of reporting permitted?

The scope of a whistleblowing report is not regulated by law. Generally, a principle of proportionality should be applied, whereby only those personal data are disclosed that are strictly necessary for the purpose of reporting (e.g., there should be no unnecessary disclosure of personal data).

12.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No, there are no limitations as to who is entitled to report under a whistleblowing program. However, according to various laws, only employees are entitled to statutory protection, not external suppliers. Employees are protected against unlawful termination of employment, discrimination and accusations of disclosing business secrets.

12.9 Are there limits as to who can be a subject of a report?

No, there are no such limitations.

12.10 Is anonymous reporting permitted?

Yes. It is stipulated by law that employees and civil servants who report corruption to authorized persons or competent state bodies are guaranteed anonymity in cases where the competent state body determines that the case at hand involves severe corruption. According to Recommendation CM/Rec (2014)7 as adopted by the Committee of Ministers of the Council of Europe on April 30, 2014, whistleblowers should be entitled to have the confidentiality of their identity maintained, subject to fair trial guarantees.

12.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes. Data transfer to other EU/EEA countries is not subject to approval but a notification is required.

12.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

Consent of employees is not required for implementing a whistleblowing program. However, as the whistleblower program may include creation of a database with personal data of the employees, consent should be obtained from employees for data collection/use/processing. In case personal data collected through the whistleblowing program are transferred outside EU/EEA countries, the consent of employees is required for such transfer.

12.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

No, the laws do not regulate this issue. However, under Recommendation CM/Rec (2014)7 adopted by the Committee of Ministers of the Council of Europe on April 30, 2014, workers and their representatives should be consulted on proposals to set up internal reporting procedures, if appropriate.

12.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

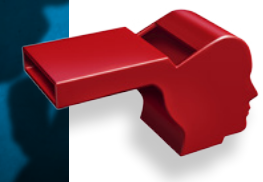
Yes. The Personal Data Protection Act and the Regulation on storage and special measures for technical protection of special categories of personal data establish a minimum threshold of protection for personal data.

The Personal Data Protection Act prescribes that personal data must be adequately protected from intentional or unintentional abuse, destruction, loss, unauthorized distortion or access. The data controller and recipient must undertake such technical and organizational measures necessary to guarantee the security and confidentiality of personal data, unintentional loss or destruction, unauthorized access, distortion, publishing and other abuse. The person employed in the department of personal data processing is obliged to sign a privacy statement. Failure to do so constitutes a misdemeanor punishable by a fine of from EUR 2,600 to EUR 5,200.

Data must be deleted once used for the purpose for which it was collected (unless a specific law stipulates a longer period of storage for specific data).

For more information, contact:

Name: Marija Mušec
Firm: Odvjetničko društvo Bardek, Lisac, Mušec, Skoko d.o.o. in cooperation with CMS Austria
Address: Ilica 1, 10000 Zagreb, Croatia
Telephone: +385 1 4825 600
Fax: +385 1 4825 601
Email: marija.musec@bmslegal.hr
Website: www.bmslegal.hr



13. CZECH REPUBLIC[11]

13.1 Applicable law and/or data protection guidelines?

The Czech Republic has not yet adopted a specific regulation on whistleblowing for commercial entities. In July 2015, the Governmental Decree No. 145/2015 Coll. was adopted, creating a legal whistleblowing framework for state employees. Previous attempts to adopt legal amendments regarding whistleblowing have not been successful.

Currently, there is a deputy parliamentary bill waiting for its first reading in the Czech House of Deputies – a bill that seeks the protection of those who report a criminal offence from potential retaliatory measures of their employer. The Czech government has stated that it would present its own bill in accordance with its Legislation Plan for 2016.

Data protection in the Czech Republic is enshrined in the Act No. 101/2000 Coll., on the Protection of Personal Data ("DPL").[12] It relies on the guidelines contained in the Article 29 Data Protection Working Party Opinion 1/2006, on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, anti-bribery, banking and financial crime.[13]

13.2 Is an English translation available?

A consolidated version of the DPL, including related amendments to other Acts, is available in English. (Please note, however, that the translation does not reflect several recent amendments to the DPL).

See www.uoou.cz/en/vismo/zobraz_dok.asp?id_ktg=1107&p1=1107

13.3 Is prior notification or approval required?

Yes, the Czech Data Protection Authority ("DPA") has to be notified prior to the collecting or processing of personal data.

13.4 Can notification or approval be filed online?

Yes. There is an online form in Czech. An English version exists, but only for reference purposes; the actual form that has to be filled in exists only in Czech.

13.5 Generally, how long does it take to get approval?

The DPA may, within 30 days from the submission of the notification, request further information or clarification in relation to the notification. If it does not act, then after the 30 day period, the notification will be deemed registered (i.e., it is not an approval process, but a registration upon notification). Usually, the DPA registers the notification in less than 30 days.

[11] The Czech Republic is a member state of the European Union. If you are interested in the EU law requirements, please refer to the section on the European Union.

[12] Accessible in Czech at: www.uoou.cz/vismo/zobraz_dok.asp?id_ktg=0&p1=0 [online 16-03-2016].

[13] Accessible at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_en.pdf [online 16-03-2016].

13.6 Contact information for Data Protection Authority?

Name:	Úřad pro ochranu osobních údajů
Address:	Pplk. Sochora 27, 170 00 Praha 7, Prague, Czech Republic
Telephone:	(Information) +420 234 665 555 or (Switchboard) +420 234 665 111
Fax:	+420 234 665 444
Email:	posta@uoou.cz
Website:	www.uoou.cz/en/

13.7 What is the scope of reporting permitted?

There is no defined scope of reporting in the applicable Czech legislation. The Article 29 Data Protection Working Party Opinion 1/2006 expressly stated that the following fields fall within the permitted scope: accounting, internal accounting controls, auditing matters, anti-bribery, banking and financial crime.

13.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No.

13.9 Are there limits as to who can be a subject of a report?

No, as long as the data subject is included in the notification to the Czech Data Protection Authority.

13.10 Is anonymous reporting permitted?

It is not prohibited. However, even though Czech law does not specifically forbid whistleblowing on an anonymous basis, anonymous reporting is not advisable for the following reasons:

First, the reported wrongdoing may amount to a criminal offense, for example, bribery or corruption. Although the report would only lead to an investigation, if it is not substantiated, the report itself may potentially be considered an offense of false accusation pursuant to s. 345 of the Act No. 40/2009 Coll., Penal Code.

Second, anonymous reporting could lead to frivolous or inconsequential reports. If the report can be linked to them and they can potentially incur liability under the Penal Code, then reporters may be more inclined to report only serious misconduct or perceived serious wrongdoing.

Otherwise, adequate safeguards must be adopted in order to minimize the risks inherent in anonymous reporting schemes (e.g., different approaches to anonymous reporting such as more checks and/or more in-depth checks of the reported information before any action potentially adverse to the person reported on is taken).

13.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes, only general rules enshrined in the data transfer provisions of the DPL apply. Data cannot be shared with foreign affiliates, e.g., company headquarters. Data can only be shared with law enforcement authorities.

13.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

The general consent of employees to the implementation of the whistleblower program is not required. The subject of whistleblowing is, in principle, not required to give consent, because the processing is necessary for the purposes of the legitimate interests pursued by the controller (employer) or by the third party or parties to whom the data are disclosed; such legitimate interests are not overridden by the interests for fundamental rights and freedoms of the data subject under the DPA.

13.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

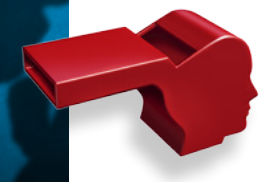
No. Works councils and unions must only be informed of the program's existence.

13.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

No. However, as pointed out above, all of the characteristics of the program, including the periods for which the personal data may be retained, must be strictly adequate to the purpose of processing. Even though there are no specific data retention periods prescribed by law, the scheme must specify for how long the data shall be retained and the controller (employer) must be prepared to justify such a period to the Czech Data Protection Authority in case it conducts an investigation.

For more information, contact:

Name: Thomas Rechberger, Ph.D.
Firm: TaylorWessing e|n|w|c advokáti v.o.s.
Tel: +420 224 81 92 16
Email: t.rechberger@taylorwessing.com
Website: www.taylorwessing.com



14. DENMARK[14]

14.1 Applicable law and/or data protection guidelines?

No, Denmark has no specific whistleblower protection laws in place.

However, according to Sections 75a and 75b of the Danish Financial Business Act, companies in the financial sector are obligated to implement a whistleblower scheme that enables employees and board members to anonymously report any violations of the financial regulations committed by the company or its employees. All companies with more than five employees that are subject to supervision by the Danish Financial Supervisory Authority must observe the mandatory requirements.

In addition, the Danish Act on Processing of Personal Data ("DPL") contains the general rules applicable to all processing of personal data, including processing of personal data in connection with whistleblower schemes.

The Danish Data Protection Agency ("DPA") has issued a set of guidelines concerning notification of whistleblower programs to the DPA. The guidelines describe the procedure to be complied with when submitting a notification to the DPA. They also set out the framework for whistleblower programs, including the requirements for and limitations regarding such programs.

Please note that the DPA generally interprets the DPL in accordance with the working papers issued by the EU Article 29 Working Party, including WP 117/2006 concerning whistleblowing schemes.

14.2 Is an English translation available?

Yes. A translation is available. See:

The Danish Act on Processing of Personal Data:
www.datatilsynet.dk/english/the-act-on-processing-of-personal-data

The whistleblowing guidelines:
www.datatilsynet.dk/english/whistleblower-systems/whistleblower-guidelines

14.3 Is prior notification or approval required?

Yes. Both notification and authorization from the DPA is required prior to implementation of a whistleblowing program. Collection and processing of personal data in connection with a whistleblowing program may not be commenced before authorization has been obtained. There is a filing fee of DKK 2,000, which is invoiced separately.

[14] Denmark is a member state of the European Union. If you are interested in the EU law requirements, please refer to the section on the European Union.

Additional notifications and authorizations are required regarding personnel administration and processing of personal data concerning business partners (if it is permitted to report on such information under the whistleblower program). Each notification and/or authorization is subject to a fee.

14.4 Can notification or approval be filed online?

Yes, notification and a request for authorization can be filed online. A specific application form for private companies must be employed. There are two different files available:

1) Standard files to be used in simple cases (most of the wording is pre-printed):

For data controllers established in Denmark:

https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Ikke-elektroniske_blanketter/FWB/WB1_Standardanmeldelse_af_whistleblowerordning_med_en_dataansvarlig_virksomhed_i_DK_-_version_1.1_nov._15.pdf

For data controllers established in third countries:

https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Ikke-elektroniske_blanketter/FWB/WB2_Standardanmeldelse_af_whistleblowerordning_med_dataansvarlig_i_et_tredjeland_-_version_1.1_nov._15.pdf

2) Special file to be used for more complex set-ups:

https://anmeld.datatilsynet.dk/frontend/1.2.pri.asp?pub=yes&myid=95540&myjour=2001-40-0003&journal=2001%2D40%2D0003&anmelder=&ord

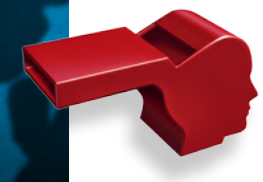
Please note that the application must be submitted in Danish.

14.5 Generally, how long does it take to get approval?

The DPA aims to process applications within five months.

14.6 Contact information for Data Protection Authority?

Name:	The Danish Data Protection Agency
Address:	Borgergade 28, 5, 1300 Copenhagen, Denmark
Telephone:	+45 33 19 32 00
Fax:	+45 33 19 32 18
Email:	dt@datatilsynet.dk
Website:	www.datatilsynet.dk



14.7 What is the scope of reporting permitted?

Only serious matters (actual or imminent) that can influence the company or group as a whole or the life or health of individuals can be reported under the whistleblower program, e.g., fraud, bribery, falsification of documents, unlawful behaviour in connection with accounting, internal accounting controls or auditing matters, corruption, and environmental violations. The DPA has specifically stated that all matters that may be reported under the U.S. Sarbanes-Oxley Act may also be reported under a whistleblower program.

Reporting on minor misconduct, e.g., bullying, absence, incompetency, issues relating to difficulties in co-operation, or violation of guidelines relating to, e.g., dress code, smoking, alcohol or use of email, are generally not permitted. Such matters should be reported through the usual channels within the company or group, such as the Human Resources department.

Furthermore, as a general rule, other sensitive personal data, such as information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or information concerning health or sex life, may not be included in the reports.

A specific assessment must be made with respect to each company/group: misconduct in one business unit might be considered minor whereas in another unit it could be considered serious.

14.8 Are there limits as to who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

Yes. Employees, management and board members, customers, suppliers and other third parties associated with the company can report through the whistleblower program.

14.9 Are there limits as to who can be a subject of a report?

Yes. Only persons affiliated with the company or the group, e.g., employees, board members, auditors, lawyers and suppliers, can be the subject of a report under the whistleblower program.

14.10 Is anonymous reporting permitted?

Yes, anonymous reporting is generally permitted. However, the DPA recommends that reporting under a whistleblower program should only be available to named informants. Furthermore, the company should make an effort to avoid anonymous reporting by informing the whistleblower that his/her identity will remain confidential unless the allegation is made in bad faith or disclosure is necessary for the purpose of further investigations or legal proceedings.

14.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes. While there are no specific restrictions when personal data is transferred within the EU/EEA, restrictions apply when personal data is transferred outside the EU/EEA. Personal data

may only be transferred to a country outside the EU/EEA provided that certain requirements are complied with, including (i) if the receiving country in question ensures an adequate level of protection, or (ii) if a legal basis (reason) is present for the transfer.

Notification of and authorization from the DPA to the transfer of the personal data to all non-EU/EEA countries will be required when sensitive data are transferred as part of a whistleblower program. Furthermore, please note that the basic data protection provisions in the DPL to the transfer itself need to be observed.

Finally, if the processing of data is carried out by way of a data processor, regardless of where the data processor is established (EU/EEA or non-EU/EEA), a data processing agreement must be entered into between the data controller and the data processor.

14.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No. The persons affected by the whistleblower program, i.e., the persons who can report and the persons who can be reported on, must, however, be informed about the implementation of the whistleblower program and the details thereof. Consequently, a whistleblower policy should be prepared prior to implementing the whistleblower program.

In addition, the DPL stipulates that the data controller must provide the data subject with certain information when collecting personal data, such as the identity of the data controller, the purpose of the processing and any further information necessary in order for the data subject to be able to safeguard his/her interests, e.g., which information has been collected, the categories of recipients, and the rules on the right of access. Therefore, information notices to the accused individual and to others on which personal data is being processed must be prepared in connection with receiving a report under the whistleblower program.

14.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

Yes. In the collective labour market, companies with more than 35 employees must appoint a Works Council consisting of members representing the employees and the management. According to the Cooperation Agreement concluded between the Confederation of Danish Employers and the Danish Confederation of Trade Unions, the Works Council must be consulted prior to implementing a whistleblower program. However, the Works Council cannot veto the implementation of a whistleblower program.

14.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

Yes.

Security Requirements

The company and any possible data processors must implement appropriate technical and organizational security measures to protect data against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure, abuse or other processing in violation of the provisions laid down in the DPL. This is relevant in particular with regard to data security requirements in connection with storage, disclosure and electronic transmission of personal data, e.g., via the internet. In the authorization issued by the DPA with respect to the whistleblower program, the DPA will lay down the requirements for security measures that must be implemented by the data controller and any processors.

Generally, this entails that the data controller (and any processor) must, on an ongoing basis, ensure compliance with, among others, the following security measures:

- Login and password procedures are in place;
- Firewall and antivirus software is up-to-date;
- Only authorized persons have access to the personal data in the whistleblowing files;
- Only persons with a work-related purpose have access to the personal data in the whistleblowing files;
- Data storage media must be stored securely so that it is not accessible to third parties;
- Buildings and systems used for data processing are secure, and only continuously updated high-quality hardware and software are used;
- There are specific logging requirements; and
- Persons who have authorized access to the personal data in the whistleblower program receive proper training, adequate instructions and guidelines on the processing of the personal data and they must be aware of the security requirements.

If a person with authorized access to the personal data processes the personal data in an EU/EEA country outside Denmark, the person in question must observe the legislation on security measures in the relevant country.

Deletion

According to the DPL, the personal data processed in connection with the whistleblower program can only be stored for as long as needed for the purpose for which it has been collected, e.g., if the report proves groundless, the personal data should be deleted immediately.

For more information, contact:

Name: Arly Carlquist or Susanne Stougaard
Firm: Bech-Bruun
Address: Langelinie Allé 35, 2100 Copenhagen, Denmark
Telephone: +45 72273462
Fax: +45 72270027
Email: ac@bechbruun.com or sus@bechbruun.com
Website: www.bechbruun.com

15. EL SALVADOR

15.1 Applicable law and/or data protection guidelines?

El Salvador has no specific whistleblower protection laws in place. Regarding data protection, there is no special law or a judicial institution, such as the "Habeas Data," for the purposes of regulating, in general, the collection, use or disclosure of personal information, whether of individuals or legal entities. However, a right to the protection of this information has been developed in a general manner by jurisprudence of the Constitutional Chamber of the Supreme Court of Justice, which relates to the individual's ability to be informed about, at the time the data is collected:

i) The kind of information that will be stored, the purpose for which the data is being obtained and processed, who the recipient of the information is, and who will administer the database in order to enable the individual to ask for any modification;

ii) The existence of databases with the purpose of enabling the individual to learn if the data is being used by third parties; and

iii) The transfer of personal data to third parties, which shall be understood not only as the individual's ability to know, in advance, the purpose of sharing the database, but also whom the recipient of the data will be, its extension, use and purpose.

This also applies, pursuant to the "Ley de Acceso a la Información Publica" (Law on Access to Public Information), which makes reference to sensitive information including personal data kept by government branches and their dependencies, autonomous institutions or any other entities managing public resources or assets.

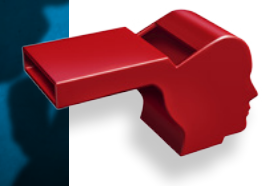
Furthermore, there are other regulations related to specific matters of data protection, such as the "Ley de Regulación de los Servicios de Información sobre el Historial de Crédito de las Personas" (Law for the Regulation of Information Services related to Individuals' Credit History), which regulates the information related to the credit history of individuals, and the "Ley de Protección al Consumidor" (Consumer Protection Act) with respect to specialized entities that render information services for financing purposes.

15.2 Is an English translation available?

No.

15.3 Is prior notification or approval required?

As indicated above, in El Salvador there are no regulations in regards to whistleblowing programs. However, any implementation of a whistleblowing program must be in accordance with the jurisprudence of the Constitutional Chamber of the Supreme Court of Justice and the



other regulations previously mentioned related to data protection. In that sense, it is important to note that the Law on Access to Public Information prescribes that the disclosure, distribution or commercialization of personal data must be authorized by the data subject.

15.4 Can notification or approval be filed online?

In regards to approval of a whistleblowing program, the Law on Access to Public Information prescribes that the consent from the data subject shall be clear and free, in writing or by any other similar means.

15.5 Generally, how long does it take to get approval?

Not applicable.

15.6 Contact information for Data Protection Authority?

Name:	Institute for the Access to Public Information
Address:	Prolongación Avenida Masferrer y Calle al Volcán No. 88, Edificio Oca Chang, Col. San Antonio Abad, San Salvador, El Salvador
Telephone:	+503 2205 3800
Fax:	+503 2205 3880
Email:	info@iaip.gob.sv
Website:	www.iaip.gob.sv

Please bear in mind that this authority is only in charge of protecting sensitive information, including personal data, kept by government branches, their dependencies, autonomous institutions or any other entities managing public resources or assets.

15.7 What is the scope of reporting permitted?

Not applicable.

15.8 Are there limits as to who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

Not applicable.

15.9 Are there limits as to who can be a subject of a report?

Not applicable.

15.10 Is anonymous reporting permitted?

Not applicable.

15.11 Are there restrictions on the transfer of data in a whistleblowing program?

Not applicable.

15.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

In El Salvador, there are no regulations on whistleblowing programs as mentioned above. However, the transfer of personal data for any whistleblowing program that eventually could be implemented, shall be in accordance with the relevant jurisprudence of the Constitutional Chamber of the Supreme Court of Justice and the other regulations previously mentioned, which are related to data protection.

15.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

No.

15.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

No.

For more information, contact:

Name: Fernando Montano
Firm: Arias & Muñoz
Address: Calle La Mascota #533, Colonia San Benito. San Salvador, El Salvador
Telephone: +503 2257-0900
Fax: +503 2257-0901
Email: fernando.montano@ariaslaw.com
Website: www.ariaslaw.com

16. EUROPEAN UNION

This chapter describes the applicable laws and guidelines of the European Union that form the basis for member state provisions on data protection. When the General Data Protection Regulation ("GDPR") goes into effect (which is expected in 2018), data protection law in the European member states will be governed by that directly applicable Regulation, which will leave considerably less room for individual national provisions than it is the case today. Check for updates on www.theworldlawgroup.com.

16.1 Applicable law and/or data protection guidelines?

Neither the current Directive 95/46/EC nor the draft GDPR contain specific provisions on whistleblowing schemes. However, guidance on whistleblowing schemes has been issued by the so-called Article 29 Working Party.

Directive 95/46/EC

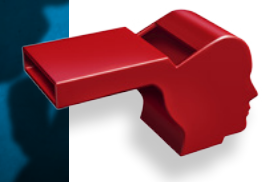
Current European data protection law is based on the Directive 95/46/EC, which was introduced in 1995. The Directive is not directly applicable to persons, bodies or companies processing personal data. EU member states are obliged to implement the provisions of the Directive into their national laws. Please see the respective chapters on the EU member state jurisdictions for further information.

Draft General Data Protection Regulation

The EU's legislative bodies are currently in the process of preparing an update to European data protection law. The General Data Protection Regulation[15] was agreed in December 2015, was officially adopted in spring 2016 and will enter into force in 2018, after a two-year transition period. The GDPR will replace Directive 95/46/EC. In contrast to the Directive, which required transposition by EU member states, the GDPR will be directly applicable in all EU member states, and aims to provide greater harmonization as well as an update of the provisions of the Directive.

Guidance from the Article 29 Working Party

The Article 29 Working Party, which is the body through which the national Data Protection Authorities of the EU member states align their polices and administrative processes, has issued guidance on the requirements for introducing whistleblower programs in its Working Paper No. 117. The paper is available for download here: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp117_en.pdf



[15] Latest draft: File ID: 2012/0011 COD, Document No. 15039/15.

16.2 Is an English translation available?

As mentioned in the response to Question 16.1 above, neither the current Directive 95/46/EC nor the GDPR contain specific provisions on whistleblowing schemes. The link provided above is the English version of the Working Party's guidance on whistleblowing programs.

16.3 Is prior notification or approval required?

Under the present Directive, notification to or approval of data protection authorities is subject to national law. Please refer to the respective chapters on the EU member states for further guidance.

According to the GDPR, the general requirement to notify data protection authorities will be abolished in favour of internal measures such as keeping a register of data processing activities, appointment of a data protection officer, or undertaking of a data protection impact assessment.

16.4 Can notification or approval be filed online?

EU law is silent on this; it is subject to member state law.

16.5 Generally, how long does it take to get approval?

EU law is silent on this; it is subject to member state law.

16.6 Contact information for Data Protection Authority?

The competent supervisory authority is the Data Protection Authority of the respective member state.

16.7 What is the scope of reporting permitted?

The Article 29 Working Party considers reporting of misconduct relating to the fields of accounting, internal accounting controls, auditing matters, bribery, banking and financial crime to be permissible. The guidance does not aim at excluding the possibility to report further issues, e.g., related to human resources, worker's health or environmental damages but is formally limited to discussing the above fields, which stem from the U.S. Sarbanes-Oxley Act. The guidance has been issued to discuss the implications of the Sarbanes-Oxley Act on EU affiliates of publicly held U.S. companies that are required to establish internal whistleblowing schemes under the Act.

16.8 Are there limits as to who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No. However, the Article 29 Working Party recommends that data controllers should carefully consider whether it might be appropriate to limit the number of persons eligible for reporting misconduct through the program given the sensitive nature of the reports and their possible impact on affected individuals.

16.9 Are there limits as to who can be a subject of a report?

No. Again, the Article 29 Working Party recommends to carefully assess whether limits are appropriate but stresses that the circumstances of each individual case are decisive.

16.10 Is anonymous reporting permitted?

Yes. The Article 29 Working Party stresses, however, that anonymous reporting is the less-preferred option. Data controllers should encourage all users to include their names with their submissions to the whistleblower system. If a user makes use of the option to report anonymously, he/she should be asked to justify why. He/she should also be informed that misusing anonymity may prevent an allegation from being fully investigated. If, despite this information, the whistleblower still wants to remain anonymous, the report should be accepted. At the same time, users have to be informed about the fact that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings resulting from the inquiries. Besides this, users should be made aware that anonymous reporting might compromise the adequacy of the inquiry.

16.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes, if the recipient is situated outside the European Economic Area and applicable local laws do not provide for an adequate level of data protection. In such cases, transfer of personal data is not permitted unless specific safeguards are adhered to (e.g., currently by means of including EU Standard Contractual Clauses). There are no exemptions for data transfers between entities belonging to the same group of companies.

Please note: The Safe Harbour has now been replaced by the Privacy Shield, which was finally approved by the European and U.S. authorities in mid-July, 2016, with an implimentation date for new applications in the U.S. of August 1, 2016. Since the European Court of Justice declared the Safe Harbour Decision invalid on October 6, 2015 (Case C-362/14), data transfers from the EU to the United States no longer could be based on the Commission's decision approving the prior Safe Harbour Principles. The European data protection authorities have been in the process of coordinating and discussing an approach for data transfers to jurisdictions that allow for extensive data access rights for national security authorities comparable to those in the U.S. Patriot Act and similar provisions. Data exporters are free to approach the competent national data protection authority or the U.S. Department of Commerce for further guidance.

16.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No. Under the Directive, processing of employees' personal data for the purposes of a whistleblower program may occur if one of the processing conditions pursuant to Art. 7 is met. According to the Article 29 Working Party, personal data may be processed if the establishment of the whistleblower program is necessary for (i) compliance with a legal obligation to which the data controller is subject (dependent on national law), or (ii) for the purposes of a legitimate interest pursued by the controller, which is subject to a balancing of interests. Such balancing of interests requires a balance to be struck between the legitimate interests of the data controller and the fundamental rights of the affected individual. These have to be taken into account when establishing a whistleblower program.

16.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

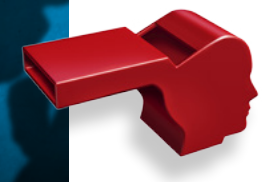
Not applicable. This is subject to national law.

16.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

The general data security requirements under the Directive apply. In particular, data controllers must adopt appropriate measures to ensure that information collected through the program is kept confidential and that a whistleblower's identity remains confidential.

For more information, contact:

Name: Christian Runte
Frim: CMS Germany
Address: Nymphenburger Straße 12, 80335 Munich, Germany
Telephone: +49 89 23807 163
Fax: +49 89 23807 40804
Email: christian.runte@cms-hs.com
Website: www.cms-hs.com



17. FINLAND[16]

17.1 Applicable law and/or data protection guidelines?

No, Finland has no specific whistleblower protection laws in place.

There is no special legislation involved with a whistleblower system but whistleblower programs have to fulfill the general requirements set forth in the Personal Data Act (523/1999), the Act on Protection of Privacy in Working Life (759/2004), and the Employment Contracts Act (55/2001).

The Data Protection Ombudsman ("DPA") has prepared guidelines for data controllers to help them in setting up such a system.

17.2 Is an English translation available?

Yes. The following translations are available but the DPA guidelines are only available in Finnish.

The Personal Data Act: www.finlex.fi/fi/laki/kaannokset/1999/en19990523.pdf

The Act on Protection of Privacy in Working Life: www.finlex.fi/fi/laki/kaannokset/2004/en20040759.pdf

17.3 Is prior notification or approval required?

No. However, there might be an obligation to notify the DPA (note: this is not an approval) if the data is being transferred outside the EU/EEA, and there is always an obligation to notify the DPA if any processing of personal data is being outsourced to a third-party service provider.

17.4 Can notification or approval be filed online?

A notification can be sent by email but it is not possible to file online.

17.5 Generally, how long does it take to get approval?

A notification has to be sent to the DPA 30 days before the action takes place. However, it usually takes up to six months to get a response from the DPA and sometimes even longer. This would not prevent a data controller from implementing a whistleblowing program.

17.6 Contact information for Data Protection Authority?

Name:	Tietosuojavaltuutetun toimisto
Address:	PL 800 00521, Helsinki, Finland
Telephone:	+358 29 56 66700
Email:	tietosuoja@om.fi
Website:	www.tietosuoja.fi/en/index.html

[16] Finland is a member state of the European Union. If you are interested in the EU law requirements, please refer to the section on the European Union.

17.7 What is the scope of reporting permitted?

An employer can only process such personal data of its employees that is necessary for the employment relationship. The appropriate purpose for processing personal data can be connected to safeguarding financial markets as well as industrial and commercial activities by preventing financial crimes related to accounting, internal accounting controls, auditing, and bribery. The appropriate purpose for processing personal data can also be to ensure that environmental and work environment regulations are followed. The purpose of an internal whistleblowing system usually is to ensure that relevant legislation, principles of corporate governance and ethical guidelines are obeyed in the company.

17.8 Are there limits as to who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

Yes. Reporting is limited to the employees, managers, and executives of the company. It does not include external suppliers.

17.9 Are there limits as to who can be a subject of a report?

No. All employees, managers, and executives can be subject of a report.

17.10 Is anonymous reporting permitted?

This is unclear under Finnish law.

There is no statute that would specifically prohibit anonymous reporting, but a person has a right to be informed about the source of information, which tends to exclude the possibility of anonymous reporting. The DPA recommends that anonymous reporting not be used.

17.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes. Data transfers outside the EU/EEA countries must follow the requirements stated in the Directive 95/46/EC and the Commission's decisions on the adequacy of the protection of personal data in third countries.

17.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No.

17.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

No. However, an employer has an obligation to handle the implementation of a whistleblowing program using a cooperation procedure. That is, if a company has fewer than 30 employees, the cooperation obligation is fulfilled when adequate information about the new system has been given to the employees. If a company has more than 30 employees, an employer has to call a

meeting in which the new procedure is explained and discussed with the employees or their representatives. It should be noted that the employees or their representatives cannot prevent or delay the introduction of a whistleblower system.

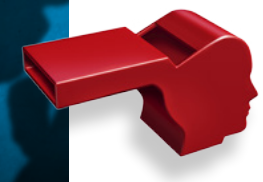
17.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

Yes. The controller must carry out the technical and organizational measures necessary for securing personal data against unauthorized access, accidental or unlawful destruction, manipulation, disclosure and transfer, and any other unlawful processing.

The DPA recommends that the data should be destroyed within two months of collecting it.

For more information, contact:

Name: Eija Warma or Anette Luomala
Firm: Castrén & Snellman Attorneys Ltd.
Address: PO Box 233 (Eteläesplanadi 14), FI-00131, Helsinki, Finland
Telephone: +358 20 7765 376
Fax: +358 20 7761 376
Email: eija.warma@castren.fi or anette.luomala@castren.fi
Website: www.castren.fi



18. FRANCE[17]

18.1 Applicable law and/or data protection guidelines?

No, France has no specific whistleblower protection laws in place.

When whistleblowing programs imply the processing of personal data, they are subject to the provisions of the French Data Protection Act.

In November 2005, the Commission Nationale de l-Informatique et des Libertés (French Data Protection Authority or hereinafter "CNIL") issued guidelines on the implementation of whistleblowing programs in compliance with the French Data Protection Act.

CNIL also published a decision (Single Authorization AU-004), that authorizes the processing of personal data implemented through a whistleblowing program that meets the requirements set out in said decision, which is available in French at www.cnil.fr/documentation/deliberations/deliberation/delib/83/.

18.2 Is an English translation available?

Yes. An official translation of the French Data Protection Act is available: www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf

18.3 Is prior notification or approval required?

Yes. Before setting up a whistleblower program, it will be necessary either to:

- Make a declaration of conformity to the Single Authorization AU-004 (simplified declaration process) if the company wishes to implement a whistleblowing program that matches the requirements set forth in the Single Authorization, or
- Apply for prior approval (standard authorization process) if the company wishes to implement a whistleblowing program that does not precisely match these requirements.

18.4 Can notification or approval be filed online?

Yes.

18.5 Generally, how long does it take to get approval?

Usually, this takes less than three months. In the event of a simplified declaration process (through the Single Authorization procedure), the acknowledgement of filing by the CNIL shall be issued within a few days or a week.

In the event of a standard authorization process, the CNIL shall issue a decision within two months from the request for approval.

[17] France is a member state of the European Union. If you are interested in the EU law requirements, please refer to the section on the European Union.

18.6 Contact information for Data Protection Authority?

Name:	Commission nationale de l'informatique et des libertés
Address:	8, rue Vivienne, CS 30223, 75083 Paris cedex 02, France
Telephone:	+33 1 5373 2222
Email:	See website
Website:	www.cnil.fr

18.7 What is the scope of the reporting permitted?

The whistleblowing programs permitted under the Single Authorization from the CNIL are those limited in scope to facts regarding the following fields, as long as the use of the data relates to the data controller's legal obligation or to its legitimate interests in these fields:

- Finance, accounting, banking (for financial institutions) and the fight against corruption;
- Antitrust law;
- Harassment and to address discrimination;
- Health, hygiene and security in the workplace; and
- Protection of the environment.

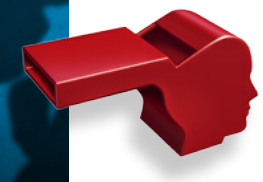
Whistleblowing programs not limited to this scope (e.g., those that include intellectual property or any violation in general that could be detrimental to the company or to the "moral or physical integrity of its employees") will not benefit from the simplified declaration process and will be reviewed by the CNIL on a case-by-case basis as to the legitimacy of the program's purposes and proportionality.

18.8 Are there limits as to who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No, there are no limits on who can make a report through the whistleblowing program. However, in the preamble to the Single Authorization, the CNIL defines whistleblowing programs as systems made available to employees. The whistleblowing programs have to define who is entitled to make a report.

18.9 Are there limits as to who can be a subject of a report?

No. However, in accordance with the principle of proportionality, the categories of persons who can be the subject of reporting must be precisely defined in the whistleblowing program.



18.10 Is anonymous reporting permitted?

Yes, anonymous reporting is tolerated as long as it is not actively encouraged by the company.

As an exception, an anonymous report may be processed provided that (i) the seriousness of the facts involved has been proven and the factual evidence is sufficiently detailed, and (ii) specific precautions are taken (e.g., prior assessment by the first recipient of the information that it is appropriate to follow up on the report within the whistleblowing system process).

18.11 Are there restrictions on the transfer of data in a whistleblowing programs?

Yes. If, in a whistleblowing program, personal data is transferred outside of the European Union, the transfer has to comply with the Data Protection Act obligations regarding international data transfers. The formal requirements vary according to the country, the designation of a Data Privacy Officer ("Correspondants informatique et libertés or "CIL") and the legal framework of the transfer.

Pursuant to the Single Authorization, such obligations under the Data Protection Act are fulfilled when:

- The recipient has entered into a transfer contract containing the standard clauses issued by the European Commission and available on the CNIL website; or
- The group to which the affected entities belong has adopted binding corporate rules which the CNIL has previously acknowledged as guaranteeing an adequate level of protection.

For these cases, and provided that the processing from which the transfer comes, complies with all the Single Authorization requirements, this also serves as authorization to transfer data.

18.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No, but employees must be informed collectively and individually of the implementation of a whistleblower program and of the transfer of their personal data.

18.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

Yes, consultation with the Works Council is required. The Works Council needs to be informed and consulted on the "means and techniques that allow control of the employees' activity" before it is implemented within the company.

Consultation with the Committee for Hygiene, Safety and Working Conditions may also be required depending on the circumstances (e.g., the implementation of a whistleblowing program has the effect or object of controlling the employees' activity, and as such could be considered as a modification of their Hygiene, Safety and Working Conditions within the meaning of the French Labour Code).

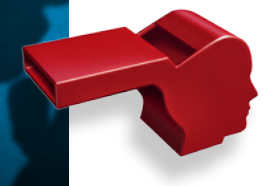
18.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

Yes. Data relating to a report found to be unsubstantiated by the entity in charge of processing such reports must be deleted immediately.

Data pertaining to a given report and reporting of facts giving rise to an investigation (or "verification") must not be stored beyond two months, unless a disciplinary procedure or legal proceedings are initiated against the person incriminated in the report or the author of an abusive/false alert. In that case, data must be deleted at the end of the procedure/proceedings.

For more information, contact:

Name: Emilie Ducorps Prouvost or Laure Marolleau
Firm: Soulier Avocats
Address: 50 Avenue de Wagram, 75017 Paris, France
Telephone: + 33 (0)1 40 54 29 29
Fax: + 33 (0) 1 40 54 29 20
Email: e.ducorpsprouvost@soulier-avocats.com or l.marolleau@soulier-avocats.com
Website: www.soulier-avocats.com



19. GERMANY[18]

19.1 Applicable law and/or data protection guidelines?

No, Germany has no specific whistleblower protection laws in place. Regarding data protection, the requirements under the German Federal Data Protection Act (Bundesdatenschutzgesetz, "BDSG") apply. Introduction of a whistleblower program typically results in collection and processing of employee data, possibly customer, supplier or other third party data as well. Regarding collection and processing of employee data, the BDSG requires that such data may only be collected or processed if deemed necessary for the performance of the employment or on the basis of a balancing of interests. Individuals whose personal data is being processed are entitled to demand access to their personal data pursuant to Sec. 34 BDSG.

Guidance by the German Data Protection Authorities

In Germany, legislative and administrative competence in data protection issues rests with the regional state level and not within the federal realm. In 2007, the Association of the German Data Protection Authorities (the so-called "Düsseldorfer Kreis") issued guidance on data protection requirements regarding whistleblower hotlines. The guidance is available here:

https://www.datenschutz-hamburg.de/uploads/media/Handreichung_Whistleblowing-Hotlines.pdf (German version only).

According to this guidance, companies should use a neutral independent party, specialized companies or law firms to operate an external whistleblower hotline to reduce the risk of misuse. Where companies turn to external service providers to outsource part of the management of the whistleblowing system, they still remain responsible for the resulting processing operations.

Guidance by the Article 29 Working Party

On a European level, the Article 29 Working Party (which is the body through which the national Data Protection Authorities of the EU member states align their polices and administrative processes), issued guidance on the requirements for introducing whistleblower programs in its Working Paper No. 117, which is available for download here: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp117_en.pdf

The recommendations of both the Düsseldorf Kreis and the Article 29 Working Party are factual and binding for the national data privacy protection authorities, and give guidance for interpretation of the data privacy protection rules. These opinions are the only official publications showing how to comply with both the U.S. Sarbanes Oxley Act and the European and German data protection requirements in Germany.

[18] Germany is a member state of the European Union. If you are interested in the EU law requirements, please refer to the section on the European Union.

19.2 Is an English translation available?

No. Only a translation of the Federal Data Protection Act is available. See:

http://www.gesetze-im-internet.de/englisch_bdsg/

19.3 Is prior notification or approval required?

No, prior notification is not required, unless companies have not appointed a data protection officer.

19.4 Can notification or approval be filed online?

Not applicable.

19.5 Generally, how long does it take to get approval?

Not applicable.

19.6 Contact information for Data Protection Authority?

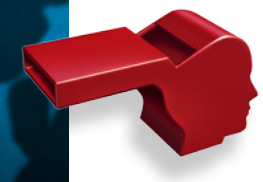
Name:	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (The Federal Commissioner for Data Protection)
Address:	Husarenstraße 30, D-53117 Bonn, Germany
Telephone:	+49 22899-7799-0
Fax:	+49 22899-7799-550
Email:	poststelle@bfdi.bund.de
Website:	www.bfdi.bund.de

Note that in Germany, supervision of compliance with data protection provisions is a regional state government responsibility. A list of the regional state government authorities can be found at: www.bfdi.bund.de/bfdi_wiki/index.php/Aufsichtsbeh%C3%B6rden_und_Landesdatenschutzbeauftragte

19.7 What is the scope of reporting permitted?

Under the BDSG, there are no legal restrictions regarding the scope of reporting in whistleblower programs.

However, the Düsseldorf Kreis and the Article 29 Working Party recommend restricting the report to serious offenses and misconduct such as discrimination, sexual harassment, bribery, corruption, betrayal of trade secrets and confidence, theft, and incorrect accounting and auditing. Reporting is not permitted for issues concerning private or intimate life, breach of non-smoking rules or allegations of bullying.



19.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No.

19.9 Are there limits on who can be subject of a report?

No. However, the company that establishes a procedure for whistleblowing programs should consider whether it would be appropriate to restrict the number of persons that can be reported on using the procedure, especially in view of the severity of alleged breaches reported. It may be advisable to open the whistleblower hotlines just for "sensitive" departments, such as sales or accounting, as recommended by the Düsseldorf Kreis and the Article 29 Working Party, and as appropriate under the principle of proportionality.

19.10 Is anonymous reporting permitted?

Yes, anonymous reporting in whistleblower programs is permitted but as a less-preferred option only. The company must encourage all users to include their names with their submissions to the whistleblowing system. If an employee makes use of the option to report anonymously, he/she should be asked to justify why. He/she should also be informed that misusing anonymity may prevent an allegation being investigated. If, despite this information, the whistleblower still wants to remain anonymous, the report should be accepted. At the same time, whistleblowers have to be informed about the fact that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings resulting from the inquiries. Besides this, the user has to be aware that anonymous reporting might compromise the success of the inquiry.

19.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes, in case the recipient is situated outside the European Economic Area and applicable local laws do not provide for an adequate level of data protection. In such cases, transfer of personal data is not permitted unless specific safeguards are adhered to (e.g., currently, by means of including EU Standard Contractual Clauses). There are no exemptions for data transfers between entities belonging to the same group of companies.

19.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No. Under German data protection law, basing data processing activities on employees' consent is viewed rather critically by many DPAs, with some German DPAs even arguing that consent may not form a legal basis, given the inevitable power imbalance governing the relationship between employee and employer.

19.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

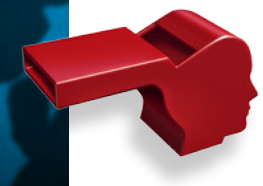
Yes, the company is obliged to negotiate on the whistleblower hotline with a Works Council (where a Works Council has been established at the respective entity). Requirements for a Works Council's participation include information on the implementation of a whistleblower program, negotiation and conclusion of an agreement. In our experience, it usually takes at least one to three months to reach an agreement.

19.14 Are there any specific computers or other security requirements, including the deletion of the reported information, for the whistleblower program?

No, but management must ensure that personal data is deleted if no longer needed. Regarding data security, the general requirements of the BDSG apply, requiring data controllers to implement adequate technical measures.

For more information, contact:

Name: Christian Runte
Frim: CMS Germany
Address: Nymphenburger Straße 12, 80335 Munich, Germany
Telephone: +49 89 23807 163
Fax: +49 89 23807 40804
Email: christian.runte@cms-hs.com
Website: www.cms-hs.com



20. GREECE[19]

20.1 Applicable law and/or data protection guidelines?

No, Greece has no specific whistleblower protection laws in place.

However, since whistleblowing programs rely in the vast majority of cases on the processing of personal data, the rules and principles of the Act Regarding Protection of Individuals with Regard to the Processing of Personal Data applies to whistleblowing programs.

20.2 Is an English translation available?

Yes. A translation of the Act Regarding Protection of Individuals with Regard to the Processing of Personal Data is available from the Hellenic Data Protection Authority's website at: www.dpa.gr/portal/page?_pageid=33,43560&_dad=portal&_schema=PORTAL

20.3 Is prior notification or approval required?

Yes. According to the general provisions of the above-mentioned Act, a company must notify the Hellenic Data Protection Authority ("DPA") in writing about the establishment and operation of a file or the commencement of data processing. Assuming that in order to set up a whistleblowing program, establishing and operating of a file or a commencing of data processing will take place, a notification to the DPA is required.

An approval from the DPA is required only when personal data that is collected for use in a whistleblowing program is transferred outside the EU/EEA.

20.4 Can notification or approval be filed online?

Yes. However, this is only available in Greek.

20.5 Generally, how long does it take to get approval?

According to the DPA, no approval is required for setting up a whistleblowing program in Greece, only a notification. However, the DPA does not directly respond to or otherwise acknowledge notifications.

20.6 Contact information for Data Protection Authority?

Name:	The Hellenic Data Protection Authority
Address:	Kifissias 1-3, 115 23 Athens, Greece
Telephone:	+30 210 6475600
Email:	contact@dpa.gr
Website:	www.dpa.gr

[19] Greece is a member state of the European Union. If you are interested in the EU law requirements, please refer to the section on the European Union.

20.7 What is the scope of reporting permitted?

The scope of reporting is limited to accounting, internal accounting controls, auditing matters, bribery, banking and financial crime.

Other issues such as discrimination or harassment should be solved though the organization's internal management or through the Department of Labour's inspectors. Companies setting up a whistleblowing program should clearly define the type of information to be disclosed through the system.

20.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

A data controller, with a positive verification by the DPA, shall determine whether such limitation or restriction is appropriate under the circumstances.

20.9 Are there limits on who can be subject of a report?

A controller, with a positive verification by the DPA, shall determine whether such limitation or restriction is appropriate under the circumstances.

20.10 Is anonymous reporting permitted?

Yes. However, it is not recommended by the DPA.

20.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes, a DPA's permit is required when personal data will be transferred outside the EU/EEA.

20.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

Yes, consent is required.

The DPA understands that, most of the time, even the written consent of the employee is not a product of free will. As a result, for a whistleblowing program or for the transfer of data in a whistleblowing program, it is crucial that this is absolutely necessary for the purposes of a legitimate interest pursued by the data controller (the employer), and on condition that such a legitimate interest evidently prevails over the right and interests of the person to whom the data refer and that his/her fundamental freedoms are not affected.

20.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

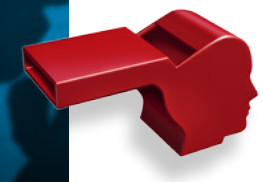
No. However, the Works Council, union or other employee representative group has to be informed about the implementation of a whistleblowing program.

20.14 Are there any specific computers or other security requirements, including the deletion of the reported information, for the whistleblower program?

No. Personal data processed by a whistleblowing scheme should be deleted promptly and usually within two months of completion of the investigation of the facts alleged in the report.

For more information, contact:

Name: Popi Papantoniou or Manto Charitos
Firm: Bahas, Gramaridis & Partners
Address: 26 Filellinon Street, Athens 105 58, Greece
Telephone: +30 210 331 8170
Fax: +30 210 331 8171
Email: p.papantoniou@bahagram.com or m.charitos@bahagram.com
Website: www.bahagram.com



21. GUATEMALA

21.1 Applicable law and/or data protection guidelines?

No, Guatemala has no specific whistleblower protection laws in place.

21.2 Is an English translation available?

Not applicable.

21.3 Is prior notification or approval required?

No, it is not necessary to seek approval from any agency or authority to set up a whistleblowing program.

21.4 Can notification or approval be filed online?

Not applicable.

21.5 Generally, how long does it take to get approval?

Not applicable.

21.6 Contact information for Data Protection Authority?

There is no specific Data Protection Authority in Guatemala.

21.7 What is the scope of reporting permitted?

There is no limit to the scope permitted for reporting in whistleblowing programs in Guatemala.

21.8 Are there limits as to who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No.

21.9 Are there limits as to who can be a subject of a report?

No.

21.10 Is anonymous reporting permitted?

Yes. Anonymous reporting is allowed and usually implemented. However, the company must obtain the information legally and guarantee the accused employee's right to be heard.

21.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes. Prior written consent of employees is required to: a) create a database with their personal information; and b) transfer the above-mentioned information to a third party.

21.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

Yes, as noted above, prior written consent of employees is required to: a) create a database with their personal information; and b) transfer the above-mentioned information to a third party.

21.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

No, there is no need for consultation with a union for the implementation of a whistleblowing program.

21.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

No.

For more information, contact:

Name: Pamela Jiménez
Firm: Arias & Muñoz
Address: Diagonal 6, 10-01 zona 10 Centro Gerencial Las Margaritas, Torre II, oficina 402-B. Ciudad de Guatemala, Guatemala, C. A.
Telephone: +502 2382 7700
Fax: +502 2382 7743
Email: pamela.jimenez@ariaslaw.com
Website: www.ariaslaw.com

22. HONDURAS

22.1 Applicable law and/or data protection guidelines?

There is no specific legislation applicable to whistleblowing programs. As for data protection laws, the Honduras Law on Transparency and Access to Public Information ("the Law") and its Regulation ("the Regulation") regulate the right to access personal or confidential information processed in public/governmental entities.

The Law states the following:

- Confidential Personal Data: Is defined as that information related to racial or ethnic origin, physical characteristics, moral or emotional characteristics, home address, phone number, email address, membership in a political organization, political ideology, religious or philosophical beliefs, health, physical or mental status, family wealth, and any other information relating to the honour, personal intimacy, and personal and family image of an individual;

- Habeas Data: Personal data will always be protected. Legal actions may be executed by the owner of personal information or the national Commissioner for Human Rights to protect against unauthorized access;

- Personal Information Databases: Individuals or entities that for work purposes create personal databases and manage confidential information may not use it without the previous consent of the owner of that information. In any case, no one is obliged to provide information containing personal data or confidential information;

- Public entities may not disclose, distribute or commercialize, or allow unauthorized access to, personal data contained within information systems developed in the exercise of their public functions unless written authorization is given by the owner of the information; and,

- Access to Personal Data: Regardless what other laws may state, only the owners of the sensitive information and their legal representatives may request public entities to provide their personal data filed in personal data systems.

Finally, it may be relevant to note that the Constitution of the Republic (Article 100) states that "everyone has the right to the inviolability and secrecy of communications, especially in the postal, telegraphic and telephonic communications, except when there is a court decision to the contrary. Corporate and personal documents may only be subject to inspection or supervision by competent authorities, as permitted by law." In addition, Article 76 guarantees honour, personal and familiar intimacy and image, and Article 183 establishes "garantia de amparo" as an action for the protection of an individual's constitutional rights.

22.2 Is an English translation available?

No, there is no English version available.

22.3 Is prior notification or approval required?

No, there is no legal requirement to notify any agency or authority to set up a whistleblower program.

22.4 Can notification or approval be filed online?

Not applicable.

22.5 Generally, how long does it take to get approval?

Not applicable.

22.6 Contact information for Data Protection Authority?

Please refer to answer 22.1. The governmental institution that supervises and controls the use of personal information in public entities is:

Name:	Instituto de Acceso a la Informacion Publica
Address:	Col. Tepeyac, Edificio Panorama, costado Sur del hospital Honduras Medical Center, calle de acceso entre el antiguo local del Restaurante La Pimentera y el antiguo local del Banco Procredit, penúltimo cubículo del lado izquierdo.
Telephone:	+504 2231-3162
Email:	marcela.sarmiento@iaip.gob.hn
Website:	www.iaip.gob.hn

22.7 What is the scope of reporting permitted?

There are no legal dispositions that restrict/limit the scope of reporting in a whistleblowing program. However, reporting on employment matters is reviewed more favourably.

22.8 Are there limits as to who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

There are no limits as to who can make a report under a whistleblowing program.

22.9 Are there limits as to who can be a subject of a report?

There are no limits as to who can be subject of a report.

22.10 Is anonymous reporting permitted?

Yes, anonymous reporting is allowed. The company must, however, obtain the information legally and guarantee the accused employee's right to be heard.

22.11 Are there restrictions on the transfer of data in a whistleblowing program?

There are no specific restrictions on the transfer of data in a whistleblowing program. For personal data purposes, Article 43 of the Regulation states that public entities may not disclose, distribute or commercialize or allow unauthorized access to personal data contained within information systems developed in the exercise of their public functions unless written authorization is given by the owner of that information. Given the latter, we strongly recommend obtaining authorization from the owner of the personal information for the transfer of data.

22.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

There is no specific legislation applicable to a whistleblower program. For personal data purposes, the Law states that individuals or entities that for work purposes create personal databases and manage confidential information may not use it without the previous consent of the owner of that information.

22.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

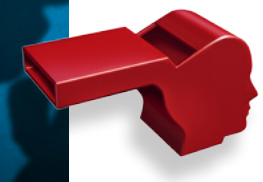
Because there is no specific legislation applicable for these purposes, there is no additional consent required by a Works Council, union or other employee representative.

22.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

There is no specific computer or other security requirements applicable to a whistleblower programs. However, it is recommended that security measures be implemented to restrict the use of any personal information databases and/or confidential information held by any third-party user.

For more information, contact:

Name: René Serrano
Firm: Arias & Muñoz
Address: Centro Comercial El Dorado 6° Piso, Boulevard Morazán, Tegucigalpa, Honduras
Telephone: +504 2221 4505
Fax: +504 2221 4522
Email: rene.serrano@ariaslaw.com
Website: www.ariaslaw.com



23. INDIA

23.1 Applicable law and/or data protection guidelines?

India has considered the adoption of a whistleblower protection law for several years. In 2014, it finally enacted a whistleblower protection law, which is still at a nascent stage. The Whistle Blowers Protection Act, 2014 ("WBP Act"), primarily seeks to protect whistleblowers, who are persons making a public-interest disclosure related to an attempt to commit or the commission of an act of corruption, misuse of power, or criminal offense by a public servant. Such public-interest disclosures against a public servant made be made by any public servant or any other person, including a non-governmental organization to the Competent Authority as defined under the WBP Act (which includes the Central and the State Vigilance Commission). The WBP Act is restricted only to disclosures against public servants.

The WBP Act received the assent of the President on May 9, 2014, and was notified in the Official Gazette of India on May 12, 2014. The provisions of the WBP Act have not, however, come into force, as the relevant notification(s) has not been issued under sub-section (3) of Section 1 of the WBP Act.

The Indian Government has subsequently proposed certain amendments to the WBP Act and has introduced the Whistleblowers Protection (Amendment) Bill, 2015, which is still under consideration by Parliament.

Additionally, the new Companies Act, 2013 ("Companies Act"), which has substantially come into effect from April 1, 2014, incorporated provisions relating to whistleblowing. Section 177(9) of the Companies Act makes it mandatory for the establishment of a "vigil mechanism" for the following classes of companies for their directors and employees to report genuine concerns or grievances:

- All listed companies;
- Companies that accept deposits from the public; and
- Companies that have borrowed money from banks and public financial institutions in excess of INR 50 crore (or five hundred million rupees).

According to Section 177(10) of the Companies Act, read with Rule 7(4) of the Companies (Meetings of Board and Its Powers) Rules, 2014, *"the vigil mechanism shall provide for adequate safeguards against victimization of a person who uses such mechanism…"* The section further provides that the establishment of a vigil mechanism has to be disclosed on the company's website and in its annual Director's Report.

In exceptional cases, the company must provide the whistleblower direct access to the chairperson of the audit committee. Additionally, the Code of Independent Directors, as set forth in Schedule IV of the Companies Act, requires independent directors to ascertain and

ensure that the company has an adequate and functional vigil mechanism, and to ensure that the interests of a person who uses such a mechanism (whistleblower) are not prejudicially affected on account of such use.

Moreover, the Securities and Exchange Board of India (SEBI) issued the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ("LODR Regulations") in September 2015, which came into effect on December 1, 2015 and apply to all entities that have listed their designated securities on recognized stock exchanges. SEBI also notified the format of a Uniform Listing Agreement on October 13, 2015, which all listed entities were required to execute within six months of the issuance of the LODR Regulations. Regulations 4(2)(d) and 22 of the LODR Regulations require listed entities to devise an effective whistleblowers mechanism and a vigil mechanism. Further, regulation 46(2)(e), Schedule II and V of the LODR Regulations contain provisions relating to the vigil mechanism and a Whistleblower Policy and its disclosures on the website and in the Annual Report of the company and review of its functioning by the Audit Committee.

Further, in relation to limited liability partnerships, Section 31 of the Limited Liability Partnership Act, 2008 provides for a "whistleblower" mechanism, which empowers the National Company Law Tribunal (NCLT) to reduce or waive any penalty levied against any partner or employee of an LLP, if it is satisfied that such a whistleblower partner or employee has provided useful information during an investigation of the affairs of an LLP relating to an offense.

Action against false or frivolous complaints

The WBP Act and the Companies Act spell out penal provisions against false or frivolous complaints.

WBP Act

Section 17 of the WBP Act sets out punishment of up to two years in prison and a fine of up to INR 30,000 for false or frivolous disclosures.

Companies Act

Under the Companies Act, in case of repeated frivolous complaints filed by a director or an employee, the Audit Committee or the director authorized may take suitable action against the concerned, including reprimand.

23.2 Is an English translation available?

- An English translation of the Whistle Blowers Protection Act, 2014 is available at: http://persmin.gov.in/DOPT/EmployeesCorner/Acts_Rules/TheWhistleBlowersProtectionAct2011.pdf
  (It is to be noted that by an amendment in 2015 to the WBP Act, the year of the WBP Act was changed from 2011 to 2014. However, the contents thereof remain the same.)

- An English translation of the Securities Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 applicable to listed companies is available at: http://www.sebi.gov.in/cms/sebi_data/attachdocs/1441284401427.pdf
- An English translation of the Companies Act, 2013 is available at www.mca.gov.in
- An English translation of the Limited Liability Partnership Act, 2008 is available at http://www.mca.gov.in/MinistryV2/llpact.html

23.3 Is prior notification or approval required?

No.

23.4 Can notification or approval be filed online?

Not applicable.

23.5 Generally, how long does it take to get approval?

Not applicable.

23.6 Contact information for Data Protection Authority?

Not applicable.

23.7 What is the scope of reporting permitted?

The WBP Act lists the nature of disclosures relating to a complaint that can be made. The complaint should relate to a disclosure against any public servant of any allegation of an attempt to commit or the commission of an act of: corruption; willful misuse of power or willful misuse of discretion; or an attempt to commit or commission of a criminal offense.

The WBP Act says that every disclosure shall be made in good faith and the person making the disclosure shall provide a personal declaration stating that he/she reasonably believes that the information disclosed by him/her and the allegation contained therein is substantially true.

Disclosures can be made in writing or by email or electronic message in accordance with the prescribed procedure, and should contain full particulars and be accompanied by supporting documents or other materials, if any.

23.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No, there are no limits on reporting under the whistleblowing program. Under the Companies Act, any employee or director can report their genuine concerns to the concerned vigil mechanism. Furthermore, the WBP Act also does not provide any kind of restriction on reporting. Any person can make a complaint.

23.9 Are there limits on who can be subject of a report?

No. Companies are free to design the whistleblower policy as they deem appropriate.

23.10 Is anonymous reporting permitted?

Anonymous reporting is not permitted under the WBP Act. Section 4(6) of the WBP Act provides that *"No action shall be taken on a public interest disclosure by the Competent Authority if the disclosure does not indicate the identity of the complainant or public servant making the public interest disclosure or if the identity of the complainant or public servant is found to be incorrect or false."*

23.11 Are there restrictions on the transfer of data in a whistleblowing program?

There are general data protection rules that require the consent of the data owner prior to sharing of data. However, there is nothing specifically dealing with data-sharing in relation to whistleblowing.

23.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No consent is required for whistleblowing. However, transfer of data requires the consent of the data provider.

23.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

No.

23.14 Are there any specific computers or other security requirements, including the deletion of the reported information, for the whistleblower program?

No.

For more information, contact:

Name: Bomi Daruwala
Firm: Vaish Associates Advocates
Address: 106, Peninsula Centre, Dr. S. S. Rao Road, Parel, Mumbai – 400012
Telephone: +91 22 4213 4101
Fax: +91 22 4213 4102
Email: bomi@vaishlaw.com
Website: www.vaishlaw.com

24. INDONESIA

24.1 Applicable law and/or data protection guidelines?

Indonesia has no consolidated or comprehensive whistleblowing program laws, regulations or guidelines in place. Whistleblower protection falls under several laws but the term "whistleblower" is not generally used in such cases and there is no direct translation of "whistleblower" in Indonesian. For the public sector, persons who report certain crimes are provided protection under Law No. 13 of 2006 on the Revision of the Protection of Witnesses and Victims. Article 10 of Law No. 13 expressly states that such persons may not be prosecuted for reporting or providing testimony. Protection for such persons is also provided by Law No. 31 of 1999 on the Eradication of Corruption as amended by Law No. 20 of 2001.

In the private sector, particularly for companies, Law No. 40 of 2007 on Limited Liability Companies provides the procedure for conducting an investigation into a company if it is alleged that the company or a member of its Board of Directors or Board of Commissioners has committed a crime that has caused either the company itself, its shareholders or a third party to suffer a loss. This is seen more as a minority-shareholder mechanism. Law No. 40 of 2007 does not, however, provide protection for persons who initiate such investigations or make reports that lead to such investigations. Companies themselves may of course have their own policies and procedures to protect whistleblowers, which may be included in their Company Regulation (i.e., Employee Handbook), Collective Labour Agreement or another policy document.

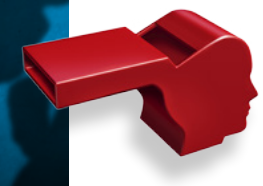
Indonesian legislation specifically on data protection consists of Law No. 11 of 2008 on Electronic Information and Transactions, and Government Regulation No. 82 of 2012 on the Implementation of Systems and Electronic Transactions, which cover non-paper based documents and information (i.e., data that is held electronically, as well as electronic transactions).

24.2 Is an English translation available?

As there are no regulations specifically relating to whistleblowing, there are no English translations.

24.3 Is prior notification or approval required?

As there are no regulations specifically relating to whistleblowing programs, there are no provisions relating to prior notification or approvals. As mentioned above, companies can include a whistleblowing program in their Company Regulation or Collective Labour Agreement or other policy documents. A Company Regulation or Collective Labour Agreement must be approved by and registered with the local Ministry of Manpower Office but this is a general requirement for the entire document and not just for any whistleblowing provisions.



24.4 Can notification or approval be filed online?

Not applicable. See above.

24.5 Generally, how long does it take to get approval?

Not applicable.

24.6 Contact information for Data Protection Authority?

Currently, Indonesia does not have a Data Protection Authority.

24.7 What is the scope of reporting permitted?

Not applicable.

24.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

Not applicable unless contractually stipulated.

24.9 Are there limits on who can be subject of a report?

Not applicable unless contractually stipulated.

24.10 Is anonymous reporting permitted?

Not applicable unless contractually stipulated.

24.11 Are there restrictions on the transfer of data in a whistleblowing program?

There is no specific law or regulation on this but under Article 26 of Law No. 11 of 2008, the use of information through electronic media that involves personal data requires the consent of the person whose data are involved, unless the data must be provided under prevailing laws.

24.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

See the response to 24.11 above. The legislation is silent on whether a whistleblowing program is exempt from the obligation to obtain the consent of the employees for the use of personal data.

24.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

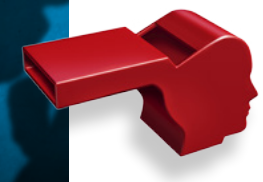
No, although discussions with employees will form part of the general preparation and finalization of both a Company Regulation and a Collective Labour Agreement.

24.14 Are there any specific computers or other security requirements, including the deletion of the reported information, for the whistleblower program?

Not applicable.

For more information, contact:

Name: Richard Cornwallis
Firm: Makarim & Taira S.
Address: Summitmas I, 16th & 17th floors, Jl. Jend. Sudirman Kav. 61-62, Jakarta 12190
Telephone: + 6221 252 1272, 520 0001
Fax: +6221 252 2750, 252 2751
Email: Richard.Cornwallis@makarim.com
Website: www.makarim.com



25. IRELAND[20]

25.1 Applicable law and/or data protection guidelines?

The Protected Disclosures Act 2014 (the "2014 Act") introduced protection for workers who "blow the whistle" about wrongdoing at work. Under the 2014 Act, workers have a right not to be dismissed or suffer a detriment at work as a result of making a "protected disclosure".

Apart from the 2014 Act, there is sectoral legislation that provides protection to persons making protected disclosures in specific sectors such as health care, health and safety, and immigration.

The Data Protection Acts 1988 – 2003 are also relevant.

25.2 Is an English translation available?

The primary language is English. See:

www.irishstatutebook.ie/eli/2014/act/14/enacted/en/pdf

25.3 Is prior notification or approval required?

No.

25.4 Can notification or approval be filed online?

Not applicable.

25.5 Generally, how long does it take to get approval?

Not applicable.

25.6 Contact information for Data Protection Authority?

Name:	Office of the Data Protection Commissioner
Address:	Canal House, Station Road, Portarlington, Co. Laois, Ireland
Telephone:	+353 1 57 868 4800
Email:	info@dataprotection.ie
Website:	www.dataprotection.ie

25.7 What is the scope of reporting permitted?

Information tending to show that one or more of the following is occurring, has occurred or is likely to occur:

- Committal of an offense;

[20] Ireland is a member state of the European Union. If you are interested in the EU law requirements, please refer to the section on the European Union.

- Failure to comply with a legal obligation;
- A miscarriage of justice;
- Danger to health and safety of an individual;
- Damage to the environment;
- Unlawful or improper use of funds and/or resources of a public body or of other public money;
- An act or omission of a public body that is oppressive, discriminatory, grossly negligent or constitutes gross mismanagement; and
- The deliberate concealment of any of the above matters.

25.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

The 2014 Act provides that workers (which include employees, contractors and agency workers) can make a protected disclosure.

25.9 Are there limits on who can be subject of a report?

No.

25.10 Is anonymous reporting permitted?

The 2014 Act provides that a person to whom a protected disclosure is made shall not disclose to another person any information that might identify the person who made the protected disclosure *unless* the person to whom the protected disclosure was made or referred:

(a) Shows he or she took all reasonable steps to avoid disclosing the information;

(b) Reasonably believes that the person who made the protected disclosure does not object to the disclosure of such information;

(c) Reasonably believes that disclosing such information is necessary for:

- The effective investigation of the relevant wrongdoing concerned;
- The prevention of serious risk to the security of the State, public health, public safety or the environment;
- The prevention of a crime or prosecution of a criminal offense; or
- The disclosure is otherwise necessary in the public interest or is required by law.

25.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes. The transfer of personal data outside EU/EEA countries must be made in accordance with the requirements stated in the Data Protection Acts 1988 and 2003.

25.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

The consent of employees is not required for the introduction of a whistleblower program.

The transfer of personal data outside the EU/EEA may be legitimized, for the purposes of the Data Protection Acts 1988 – 2003, based upon consent of the data subject concerned (though there are other bases on which to legitimize such transfer). The Data Protection Commissioner has questioned whether consent from employees is a valid consent in all cases due to the nature of the employer/employee relationship.

25.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

No.

25.14 Are there any specific computers or other security requirements, including the deletion of the reported information, for the whistleblower program?

Apart from the general provisions of the Data Protections Acts 1988 – 2003 (e.g., with respect to adequate security measures and the requirement to keep personal data for no longer than necessary), there are no specific provisions around the deletion of reported information.

For more information, contact:

Name: Robert McDonagh or Elizabeth Ryan
Firm: Mason Hayes & Curran
Address: South Bank House, Barrow Street, Dublin 4, Ireland
Telephone: +353 1 614 5000
Fax: +353 1 614 5001
Email: rmcdonagh@mhc.ie or eryan@mhc.ie
Website: www.mhc.ie

26. ISRAEL

26.1 Applicable law and/or data protection guidelines?

The Protection of Employees Law (Exposure of Offenses of Unethical Conduct and Improper Administration) Law 5757-1997 (the "Protection of Employees Law") is the main law that protects whistleblowing employees in Israel.

In addition, Israel has general legislation with respect to protection of privacy entitled, "The Protection of Privacy Law, 1981" (the "Privacy Law").

26.2 Is an English translation available?

No.

26.3 Is prior notification or approval required?

No. However, the program must comply with the above Protection of Employees Law, and if applicable, under the specific circumstances, the Privacy Law.

26.4 Can notification or approval be filed online?

Not applicable.

26.5 Generally, how long does it take to get approval?

Not applicable.

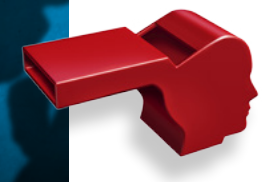
26.6 Contact information for Data Protection Authority?

Name:	The Israeli Law, Information and Technology Authority
Address:	The Government Campus, 9th floor, 125 Begin Road, Tel Aviv, Israel (Mailing address: P.O. Box 7360, Tel Aviv 61072, Israel)
Telephone:	+972-3-763-4050
Email:	ILITA@justice.gov.il
Website:	http://www.justice.gov.il/En/Units/ILITA/Pages/default.aspx

26.7 What is the scope of reporting permitted?

Under the Protection of Employees Law, there are no specific limitations on the scope of reporting regarding whistleblowers. However, protection under the Protection of Employees Law will be given, subject to meeting certain conditions, such as:

(a) The complaint was brought by the complainant in good faith, or the complainant assisted in the filing of the complaint in good faith;



(b) The complaint was submitted in relation to the commission of an offense under any enactment in the workplace or in connection with the breach of legislation at the workplace or a breach of any legislation relating to the employee's work, or the employer's field of business activity, or in a public body; also, where the complaint was filed in regard to unethical conduct or improper administration; and

(c) The complaint was filed with an authority competent to receive complaints or competent to investigate the matter that is the subject of the complaint.

26.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No. However, only employees will be given the protection granted under the Protection of Employees Law.

26.9 Are there limits on who can be subject of a report?

No, although there are limitations on the subject of the complaint, which is in accordance with the Protection of Employees Law, as described above.

26.10 Is anonymous reporting permitted?

According to the Protection of Employees Law, there is no specific prohibition on anonymous reporting, although it is unclear what kind or protection the whistleblower would receive in such case.

26.11 Are there restrictions on the transfer of data in a whistleblowing program?

No. Notwithstanding, it should be noted that the general rules and restrictions of the Privacy Law shall apply with respect to any transfer of personal data, including receiving the required consents for such specific transfer, if applicable, and if necessary amending the registration of the applicable database.

Specific regulations have been enacted with respect to the transfer of data from a database in Israel to one outside of Israel, entitled, "The Protection of Privacy Regulations (the Transfer of Information to a Database outside the State Borders), 2001" (the "Transfer Regulations").

1. The Transfer Regulations impose restrictions in addition to all other restrictions on transfers of data that appear in the Privacy Law. The Transfer Regulations prohibit the transfer of information from a database in Israel to a database located abroad, unless the receiving country ensures a level of protection of information that equals or exceeds the level of protection provided for under Israeli law.

2. Notwithstanding the foregoing, the Transfer Regulations permit the transfer of information from a database in Israel to a database abroad, upon the fulfilment of any one of the following, inter alia, conditions:

   (a) Receipt of a consent to the transfer of the information from the person who is the subject of the information;

   (b) The information is being transferred to a corporation under the control of the owner of the Israeli database and it has ensured the protection of privacy following the transfer;

   (c) The information is being transferred to someone who has undertaken to fulfill the conditions laid down in Israel for the maintenance and use of the information, and any changes necessary have been made;

   (d) Transferring the information is essential for the defense of public welfare and security;

   (e) The information is being transferred to a database in a country in which any one of the following conditions exist:

      (i) It is a party to the European Convention for the Protection of Individuals in connection with automatic processing of sensitive information;

      (ii) It receives information from member states in the European Union, under the same conditions of receipt;

      (iii) The Registrar of Databases has notified with respect to the country, in a notification that has been published in the Official Gazette, that there exists in such country a designated authority to protect privacy and that it has reached an arrangement for cooperation with that authority (to date there has been no such notification).

In addition to the fulfilment of the above conditions, (with respect to both points 1 and 2 above), the recipient of the data must undertake to ensure the privacy of the person to whom the information relates, and not to transfer the information to any person/entity.

In addition, we would note that, according to the Privacy Law, there are several defenses that might apply. Such defenses might apply in cases where the defendant or the accused committed the infringement in good faith in the following circumstance:

   (a) The infringement was committed under circumstances under which the infringer was under a legal, moral, social or professional obligation to commit it;

   (b) The infringement was committed in defense of a legitimate personal interest of the infringer;

   (c) The infringement was committed in the lawful pursuit of the infringer's occupation and in the ordinary course of his/her work, provided that it was not committed by way of publication.

26.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

Determining whether or not employee consent is required is subject to the specific circumstances of the matter and to the application of the Privacy Law with respect to such circumstances. If an employee's consent will be required, such consent would have to be explicit.

26.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

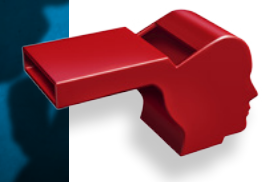
Any specific advice in this regard should be given based on the specific circumstances of the case at hand, including the specific terms of the program to be implemented and the terms of any collective agreements that are applicable to the workplace. As a general rule, consultation with the employees' representative (if one exists) is required if the employer plans to make changes in employment terms or structural changes at the workplace, which may affect the employees' conditions of employment or in general any change in previous agreements between the parties.

26.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

No. As mentioned above, there are no specific privacy-oriented rules or legislation with respect to whistleblower programs in Israel. Therefore, the general provisions of the Privacy Law shall apply also on whistleblowing programs.

For more information, contact:

Name	Nurit Dagan or Moria Tam-Harshoshanim
Firm:	Herzog, Fox & Neeman Law Office
Address:	Asia House, 4 Weizmann St, Tel Aviv 64239, Israel
Telephone:	+972 3 692 7424 and +972 3 692 5530
Fax:	+972 3 696 6464
Website:	www.hfn.co.il
Email:	dagan@hfn.co.il or tam@hfn.co.il



27. ITALY[21]

27.1 Applicable law and/or data protection guidelines?

Italy has very recently issued specific provisions regarding whistleblower protection and guidelines exclusively with reference to the banking and financial sector by means of the approval of Legislative Decree No. 72 of May 12, 2015, in force from June 27, 2015, which partially amended Italy's Consolidated Law on Banking and Consolidated Law on Finance by introducing whistleblowing and reporting systems both internal to companies operating in these sectors and to the relevant supervisory authorities, for violations of the provisions related to banking and financial activity. To this extent, the supervisory authority, the Bank of Italy, implemented specific guidelines on July 21, 2015.

In addition, and in relation to the public sector, Law No. 190 of November 6, 2012 has incidentally affirmed the protection of the public employee who denounces or reports illicit behaviours that become known during his/her employment relationship.

However, currently there are no Italian general whistleblower protection laws in place, nor any data protection guidelines in this respect. However, on December 10, 2009, the Italian Data Protection Authority ("DPA") addressed both the Italian Parliament and Government with a recommendation to enact adequate legal provisions aimed at regulating the use of whistleblowing programs and, in general, of other systems reporting alleged violations by a business organization (the "Recommendation"). However, no legislative or governmental initiative followed the Recommendation except for the specific provisions applying to the above-mentioned banking and financial sectors and, marginally, the public sector. Thus, for the time being, any whistleblowing program has to be governed by the existing and general privacy rules, including the Italian Privacy Code. Please note that it is normal to make reference also to the Article 29 Working Party Guidelines on whistleblowing programs as chapters about other EU countries do in this guide.

27.2 Is an English translation available?

No. Only a translation of the Privacy Code is available at:
www.garanteprivacy.it/garante/document?ID=1219452

27.3 Is prior notification or approval required?

Although still not officially translated into a legal provision, prior notification to the DPA is strongly recommended, since the Italian Data Protection Act imposes the obligation of notifying those processing operations concerning "data stored in ad-hoc data banks managed by electronic means in connection with appropriate performance of obligations, and unlawful and/or fraudulent conduct."

[21] Italy is a member state of the European Union. If you are interested in the EU law requirements, please refer to the section on the European Union.

27.4 Can notification or approval be filed online?

Yes, by means of the specific online notification form provided on the DPA's website: https://web.garanteprivacy.it/rgt/NotificaInserimento.php?h_act=U&x=65.52115177933352

27.5 Generally, how long does it take to get approval?

No approval is required once the notification is filed.

27.6 Contact information for Data Protection Authority?

Name.	Garante per la protezione dei dati personali
Address:	Piazza di Monte Citorio n. 121, 00186 Rome, Italy
Telephone:	+39 06 69677 1
Fax:	+39 06 69677 785
Email:	garante@garanteprivacy.it
Website:	www.garanteprivacy.it

27.7 What is the scope of reporting permitted?

Under the Italian Data Protection Act, there are no legal restrictions regarding the scope of reporting in whistleblower programs. Usually, beyond the specific whistleblowing provisions issued for the banking and financial sectors, the principles and the procedures set forth by the EU Article 29 Working Party (Opinion 1/2006 or "the Guidelines") are observed by companies that want to implement a whistleblowing system. These Guidelines recommend restricting reporting to serious offenses and misconduct such as discrimination, sexual harassment, bribery, corruption, betrayal of trade secrets and confidence, theft, incorrect accounting and auditing. However, reporting is not permitted (according the Italian Statute of Work, L 300/70) in areas concerning private or intimate life, breach of non-smoking rules or allegations of bullying.

27.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No. There are no legal limits except the rules set forth by the Article 29 WP. The specific whistleblowing provisions issued for the banking and financial sectors generically refer to the "personnel" meaning, according to the guidelines from the Bank of Italy, employees and those who operate in the context of a relationship determining their inclusion in the entity's organizational structure, which is different from the subordinate employment relationship.

27.9 Are there limits on who can be subject of a report?

No, there are no legal restrictions, except under the rules set forth by the Article 29 Working Party.

27.10 Is anonymous reporting permitted?

Yes.

27.11 Are there restrictions on the transfer of data in a whistleblowing program?

No. However, all of the ordinary EU restrictions applicable to any cross-border data transfer apply.

27.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

It is unclear under the current legislation. Usually, companies do not ask for consent, relying on an exemption from consent.

27.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

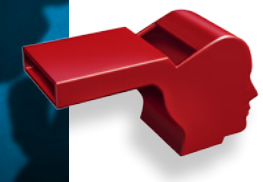
No. Nonetheless, depending on the way in which the relevant whistleblowing program is adopted and managed, a consultation with the Works Council may be recommended.

27.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

No, but general rules apply. From a general point of view, personal data to be processed must be kept and controlled in such a way as to protect against, by means of suitable preventative security measures, the risk of data destruction or loss, whether by accident or not, of unauthorized access to the data or of processing operations that are either unlawful or inconsistent with the purposes for which the data have been collected.

For more information, contact:

Name: Daniele Vecchi or Melissa Marchese
Firm: Gianni, Origoni, Grippo, Cappelli & Partners
Address: Piazza Belgioioso, 2 20121, Milan, Italy
Telephone: +39 02 7637 41
Fax: +39 02 7600 9628
Email: dvecchi@gop.it or mmarchese@gop.it
Website: www.gop.it



28. JAPAN

28.1 Applicable law and/or data protection guidelines?

Japan has a specific whistleblower protection law in place called the Whistleblower Protection Act (Law No. 122, 2004). Protection of personal data is regulated under the Act on the Protection of Personal Information ("APPI"), separately from the whistleblower protection issue.

28.2 Is an English translation available?

Yes. A translation is available at: www.cas.go.jp/jp/seisaku/hourei/data/WPA.pdf.

28.3 Is prior notification or approval required?

No.

28.4 Can notification or approval be filed online?

Not applicable.

28.5 Generally, how long does it take to get approval?

Not applicable.

28.6 Contact information for Data Protection Authority?

Not applicable.

28.7 What is the scope of reporting permitted?

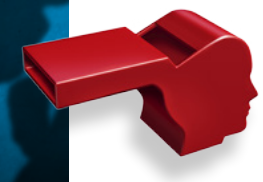
The scope of reporting permitted is limited to facts of criminal activities set forth in laws that are specifically listed or facts relevant to violation of laws related to such criminal activities. As of September 2015, 453 laws are specifically listed.

28.8 Are there limits on who can make a report under a whistleblowing program? (e.g., only managers and executives? Other employees? Suppliers?)

Yes. Only "workers" as defined under the Labour Standards Act can make a report.

28.9 Are there limits on who can be a subject of a report?

Yes. Only the entity or individual to whom the labour is provided, and officers, employees, agents and others of such entity or individual can be the subject of a report.



28.10 Is anonymous reporting permitted?

In principle, anonymous reporting is not protected under the Whistleblower Protection Act, but depending on the case, such as when the anonymous reporter is identified at a later time, anonymous reporting could also be protected under the Act.

28.11 Are there restrictions on the transfer of data in a whistleblowing program?

No. However, transfers of data are subject to restrictions under the APPI.

28.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No. The consent of employees is not required under the Whistleblower Protection Act. But transfer of personal information to third parties without obtaining prior consent is prohibited in principle with certain exceptions under the APPI.

28.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

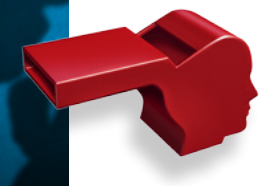
No.

28.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

No.

For more information, contact:

Name: Hitoshi Sakai
Firm: City-Yuwa Partners
Address: Marunouchi Mitsui Building, 2-2-2 Marunouchi, Chiyoda-ku, Tokyo, 100-0005
Telephone: + 81 3 6212 5642
Fax: + 81 3 6212 5700
Email: hitoshi.sakai@city-yuwa.com
Website: www.city-yuwa.com



29. LUXEMBOURG[22]

29.1 Applicable law and/or data protection guidelines?

The Law of August 2, 2002 on the Protection of Persons with regard to the Processing of Personal Data as amended ("the DPL") applies to whistleblowing schemes.

The Luxembourg Data Protection Authority (the "DPA") has also delivered some guidelines focusing on whistleblowing systems ("the Guidelines"). These guidelines were inspired by Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes issued by the Article 29 Data Protection Working Party ("the Opinion").

Whistleblowing schemes are also subject to compliance with Articles L. 271-1 et seq. of the Labour Code. Under these provisions, the employee is protected against reprisals if he/she reports (or testifies in litigation involving) acts of corruption, illegal acquisition of interests or influence peddling committed by a fellow employee, his/her manager or employer.

29.2 Is an English translation available?

A non-official English translation of the DPL is available at http://www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi02082002_en.pdf.

Note, however, that this not the latest coordinated version of the DPL (no complete coordinated text exists), which has been amended twice since 2007 (in August 2011 and July 2014). But these amendments only concern the status and the appointment of the DPA's members and the right for patients to access their medical data.

The EU Article 29 Working Party Opinion is available in English at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_en.pdf.

29.3 Is prior notification or approval required?

A notification has to be filed with the DPA prior to any data processing undertaken within the context of a whistleblowing system.

Where the whistleblowing system would imply data transfers outside of the European Union to countries that do not offer an adequate level of protection, a prior authorization would be required (see response to Questions 29.11 & 29.12 below).

29.4 Can notification or approval be filed online?

A notification can be filed online.

An application for authorization cannot be filed online. It has to be addressed via post to the DPA.

[22] Luxembourg is a member state of the European Union. If you are interested in the EU law requirements, please refer to the section on the European Union.

29.5 Generally, how long does it take to get approval?

Concerning notifications, the acknowledgement of receipt/filing shall be issued within a few weeks.

Regarding approvals, it could take between six months and one year to obtain such approval.

29.6 Contact information for Data Protection Authority?

Name:	Commission Nationale pour la Protection des Données
Address:	1, avenue du Rock'n'Roll, 4361 Esch-sur-Alzette, Luxembourg
Telephone:	+352 26 1060 1
Fax:	+352 26 1060 29
Website:	www.cnpd.public.lu

29.7 What is the scope of reporting permitted?

According to the Guidelines and the Opinion, whistleblowing processes may only be carried out in the fields of accounting, internal accounting controls, banking matters and bribery.

29.8 Are there limits as to who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

According to the Opinion and the Guidelines, the company responsible for a whistleblowing program should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconducts in the light of the seriousness of the alleged offenses to be reported.

Therefore, there are no precise limits as to the persons entitled to make a report under a whistleblowing program. Managers responsible for whistleblowing systems shall determine the persons qualified to make such reports on a case-by-case basis.

29.9 Are there limits as to who can be a subject of a report?

According to the Opinion and the Guidelines, the company responsible for the whistleblowing schemes should carefully assess whether it might be appropriate to limit the persons who may be reported on through the whistleblowing scheme.

Therefore, there are no specific limits as to the persons that may be the subject of a report in the context of a whistleblowing program. Managers responsible for whistleblowing systems should determine the persons that may be reported on a case-by-case basis.

29.10 Is anonymous reporting permitted?

According to the Opinion and the Guidelines, only identified reports should be communicated through whistleblowing schemes. However, anonymous reports may be filed through the scheme and acted upon, but as an exception to the rule and under the following conditions:

- Whistleblowing systems should be built in such a way that they do not encourage anonymous reporting as the usual way to make a complaint;
- Companies should not advertise the fact that anonymous reports may be made through the system. On the contrary, whistleblowing schemes should ensure that the identity of the whistleblower is processed under conditions of confidentiality;
- An individual who intends to report to a whistleblowing system should be aware that he/she will not suffer due to his/her action. For that reason, the individual should be informed, at the time of establishing first contact with the system, that his/her identity will be kept confidential at all the stages of the process and, in particular, will not be disclosed to third parties, either to the incriminated person or to the employee's line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted;
- Whistleblowers have to be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of the enquiry conducted via the whistleblowing scheme;
- The processing of anonymous reports must be subject to special caution. Such caution would, for instance, require examination by the first recipient of the report with regard to its admission and the appropriateness of its circulation within the framework of the scheme;
- Anonymous reports may be investigated and processed with greater speed than confidential complaints because of the risk of misuse.

29.11 Are there restrictions on the transfer of data in a whistleblowing program?

This depends on the country where personal data is transferred.

The transfer of personal data to a country within the European Union (EU), in the European Economic Area ("EEA"), or to a country that is deemed to offer an adequate level of protection by the DPA or by the European Commission (such as Canada, Argentina or New Zealand) is not subject to any particular conditions as long as it complies with the general condition of legitimacy, adequacy and lawfulness of data processing.

However, any transfer of employees' personal data to a country that does not offer an adequate level of protection must, in addition to the general conditions mentioned above, first be authorized by the DPA on the basis of EU Standard Contractual Clauses or Binding Corporate Rules.

29.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

The consent of employees is not required for a whistleblowing program that does not involve any data transfers in countries that do not offer an adequate level of protection. However, the employees must be informed of the data processing undertaken within the context of the whistleblowing program. Such information must include, among other things, the identity of the data controller, the categories of personal data to be processed, the categories of recipients of such data, the reasons for such data processing, and the right of access to and rectification of the data.

In situations where the whistleblowing program would imply data transfers outside of the EU to countries that do not offer an adequate level of protection, the consent of employees is not mandatory but the employees must be informed of any data processing undertaken within the context of the whistleblowing program, and the employer must obtain an authorization from the DPA prior to the data transfers (please see the response to Question 29.11).

29.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

If the employer decides to implement the whistleblowing policy in the company, this decision (as it will be considered as part of the company's internal regulation), has to be taken together with the employee representative bodies (either the staff delegation or the Works Council depending on the numbers of employees employed by the company). The staff delegation (or the Works Council) does in this case have a co-decision right.

If, however, an employee wants to denounce another employee of the company after the implementation of the whistleblowing policy, neither prior information of the employee representative bodies nor their consent will be required.

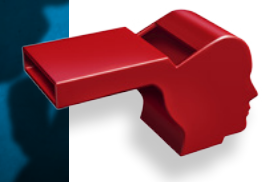
29.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblowing program?

The organization responsible for a whistleblowing scheme shall take all technical and organizational measures to preserve the security of the data when it is gathered, circulated or maintained. Its aim is to protect data from accidental or unlawful destruction or accidental loss and unauthorized disclosure or access.

The reports may be collected by any data processing means, whether electronic or not. Such means should be dedicated to the whistleblowing system in order to prevent any diversion from its original purpose and for confidentiality.

For more information, contact:

Name: Héloïse Bock
Firm: Arendt & Medernach S.A.
Address: 41A, avenue J.F. Kennedy, L-2082 Luxembourg
Telephone: +352 40 7878 321
Fax: +352 40 7804 609
Email: Heloise.Bock@arendt.com
Website: www.arendt.com



30. MALAYSIA

30.1 Applicable law and/or data protection guidelines?

Yes, Malaysia has specific whistleblower protection laws in place. Malaysia's whistleblower protection laws are pursuant to the Whistleblower Protection Act 2010.

30.2 Is an English translation available?

Yes, a translation is available at the official portal of the Legal Affairs Division (BHEUU) of the Prime Minister's Department at: www.bheuu.gov.my/portal/pdf/Akta/Act%20711.pdf

30.3 Is prior notification or approval required?

No.

30.4 Can notification or approval be filed online?

Not applicable.

30.5 Generally, how long does it take to get approval?

Not applicable.

30.6 Contact information for Data Protection Authority?

The Department of Personal Data Protection (JPDP), an agency under the Ministry of Communications and Multimedia was established in 2011.

Name:	Personal Data Protection Department
Address:	Level 6, Kompleks KPKK, Lot 4G9, Persiaran Perdana, Presint 4, Pusat Pentadbiran Kerajaan Persekutuan, 62100 Putrajaya
Telephone:	+6 03 8911 7901
Email:	pcpdp@kpkk.gov.my
Website:	www.pdp.gov.my/index.php/en/

30.7 What is the scope of reporting permitted?

A report can be made by any person against any conduct which, if proved, constitutes a disciplinary or criminal offense. However, a report can only be made to an enforcement agency, i.e., a ministry, department, agency, division, section or unit set up by the government or under federal/state law having investigation and enforcement functions. The five main key enforcement agencies are the Royal Malaysian Police, the Royal Malaysian Customs, the Road Transport Department, the Malaysian Anti-Corruption Commission and the Immigration Department.

30.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No. Reports can be made by any person against any conduct, which if proved, constitutes a disciplinary offense or a criminal offense.

30.9 Are there limits on who can be a subject of a report?

No. Anyone can be a subject of a report.

30.10 Is anonymous reporting permitted?

Yes.

30.11 Are there restrictions on the transfer of data in a whistleblowing program?

No. The data collected by the enforcement agency is to be used for investigation purposes and to determine if disciplinary action or prosecution is to be taken against the subject of the complaint.

30.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No.

30.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

Not applicable.

30.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

Not applicable.

For more information, contact:

Name: Shanti Mogan
Firm: Shearn Delamore & Co.
Address: 7th Floor Wisma Hamzah Kwong Hing, No 1 Leboh Ampang, 50100 Kuala Lumpur, Malaysia
Telephone: +603 2027 2921
Fax: +603 2034 2763
Email: shanti@shearndelamore.com
Website: www.shearndelamore.com

31. MEXICO

31.1 Applicable law and/or data protection guidelines?

Mexico does not have a comprehensive whistleblower protection law in place. However, certain federal laws in Mexico contain provisions with whistleblower mechanisms for the public and private sectors. Below is a brief description of those we consider most relevant:

- The Federal Anti-corruption Law on Public Procurement ("Ley Federal Anticorrupciónen Contrataciones Públicas" – "Anti-corruption Law"), published in the Federal Official Gazette on June 11, 2012, which establishes certain whistleblower mechanisms to report irregular conduct carried out, directly or indirectly:

  (i) By any individual or entity with the intention to influence the decision of a Mexican public officer involved in a federal public procurement (such as acquisitions, lease and service contracts, or public constructions and services related therewith) ("Mexican Corruption Conduct"); or

  (ii) By any Mexican individual or entity with the purpose of influencing the decision of any foreign public officer under any procedure carried out abroad in connection with public foreign procurements (acquisitions, lease and service contracts, or public constructions and the services related therewith) or the granting or renewal of any permit, authorization or concession ("Foreign Corruption Conduct").

- The Federal Law on Economic Competition ("Ley Federal de Competencia Económica" - "Antitrust Law") allows economic agents or individuals to provide information to the Antitrust Agency ("Comisión Federal de Competencia Económica") to begin a proceeding against absolute monopolistic practices.

Any processing of personal data under the Anticorruption Law and Antitrust Law shall comply with those data protection provisions referred to in Chapter IV, Title One of the Federal Law for Transparency and Access to Public Governmental Information, its Regulations and the guidelines ("Transparency Laws") issued by the National Institute of Transparency, Information Access, and Personal Data Protection ("Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales" or "INAI"). In the event that a company wishes to establish an internal whistleblowing program, and it would involve any processing of personal data, such mechanisms shall comply with the Federal Law for the Protection of Personal Data in Possession of Private Parties and its regulations ("Data Protection Laws").

31.2 Is an English translation available?

No.

31.3 Is prior notification or approval required?

Not applicable.

31.4 Can notification or approval be filed online?

Not applicable.

31.5 Generally, how long does it take to get approval?

Not applicable.

31.6 Contact information for Data Protection Authority?

Name:	National Institute of Transparency, Information Access, and Personal Data Protection
Address:	Insurgentes Sur No. 3211, Colonia Insurgentes, Cuicuilco, Delegación Coyoacán, Zip Code 04530, Distrito Federal, México
Telephone:	+52 01 800 8354324
Email:	atencion@ifai.org.mx
Website:	www.ifai.org.mx

31.7 What is the scope of reporting permitted?

Currently, external reports before public agencies are limited to those sectors regulated by the corresponding legislation (e.g., the Anti-corruption Law or the Antitrust Law). In the case of the Anti-corruption Law, the reports are limited to corruption activities. In the case of the Antitrust Law, reports shall be about absolute monopolistic practices.

31.8 Are there limits as to who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

Limitations will depend on the law under which the report is filed. In the event of reports under the Anti-corruption Law, there are no limitations on the subject that may file the report, even foreign "estates or organisms" may file a report about a Foreign Corruption Conduct.

In case of whistleblowing programs under the Antitrust Law, such would be limited to any economic agent who has committed or is committing an absolute monopolistic practice or has participated directly on behalf of or in representation of legal entities in such practices, as well as those economic agents or individuals who have contributed, caused, induced or participated in the commission of an absolute monopolistic practice (i.e., "Absolute Monopolistic Agents").

A whistleblowing program implemented by a private entity may establish, at its discretion, the terms in which someone may file a report under its whistleblowing program, to the extent that the program does not infringe any other law.

31.9 Are there limits as to who can be a subject of a report?

In terms of the Anti-corruption Law, any individual can be a subject of a Mexican Corruption Conduct report. However, if the report is related to a Foreign Corruption Conduct, it may only involve acts of individuals with Mexican nationality or entities established in Mexico.

Under the Antitrust Law, only Absolute Monopolistic Agents can be subject to a report.

As previously mentioned, in whistleblowing programs implemented by private entities, such entities are free to establish who can be a subject of a report under its whistleblowing program as long as they do not infringe any Mexican law.

31.10 Is anonymous reporting permitted?

Yes. Anonymous reporting is allowed through the means established by the Anti-corruption Law for that effect.

Anonymous reporting is not allowed under the Antitrust Law; notwithstanding this, the identity of the economic agent or individual that files the report will be kept confidential.

Since the rules and procedures of internal whistleblowing programs created by private entities are not governed by specific regulation, each relevant entity may determine, at its discretion, if the reports can be filed anonymously.

31.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes. In the case of external whistleblowing programs carried out before a governmental agency, such as those under the Anti-corruption Law and Antitrust Law, the identity of the whistleblower shall be kept as confidential. In addition, any personal data processed by the corresponding governmental body during any whistleblowing proceeding under said laws shall be transferred in accordance with provisions of the Transparency Laws. In the case of a whistleblower proceeding, consent of the data subject is not required for the transfer of personal data provided that the data is used by the corresponding governmental agency that is carrying out the investigation proceeding under the Anti-corruption Law.

In the event of whistleblowing programs implemented by private entities, the transfer of personal data shall comply with the Data Protection Laws.

31.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

The consent of data subjects, including employees, would not be applicable when the corresponding laws create whistleblowing mechanisms. To implement an internal whistleblowing program, consent is not required; however, if the entity wishes to make such a program binding, it would have to inform employees of such policy and obtain their consent, perhaps as a part of an internal regulation, code or policy applicable to all employees.

Unless exempted by the Transparency Laws and Data Protection Laws, any transfer of personal data would require the consent of the data subject including employees. Therefore, the transfer of personal data within a whistleblowing mechanism handled by a governmental agency or an internal whistleblowing program should be analyzed on a case-by-case basis.

31.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

No.

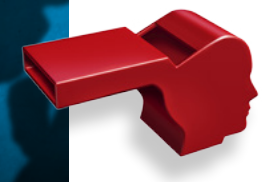
31.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

Yes. Pursuant to Guidelines 30 through 37 of the Guidelines for the Protection of Personal Data, any governmental body that maintains a database with personal data shall adopt security measures to avoid any unauthorized alteration, loss, consultation, copying or deletion of personal data, and therefore guarantee the security and confidentiality of such data. It should be noted that such measures and procedures are not exclusive of personal data used in whistleblower proceedings, but applicable to any database held by a governmental body.

Internal whistleblowing programs implemented by private entities shall comply with security provisions of the Data Protection Laws and may follow those recommendations on security of personal data published by the INAI in the Federal Official Gazette on 30 October 2013.

For more information, contact:

Name: César G. Cruz Ayala or Diego R. Acosta Chin
Firm: Santamarina y Steta
Address: Ricardo Margain Zozaya 335, Piso 7, Col. Valle del Campestre, 66265 San Pedro Garza García, N.L., (Monterrey) México
Telephone: +52 81 8133 6002 or +52 81 8133 6018
Fax: +52 81 8368 0111
Email: ccruz@s-s.mx or dacosta@s-s.mx
Website: www.s-s.mx/site/eng



32. MONGOLIA

32.1 Applicable law and/or data protection guidelines?

Mongolia has no specific whistleblower protection laws in place. A similar concept to whistleblower protection is the protection of a police informant who informs the police of potential crimes (i.e., someone preparing to commit a crime) or crimes that have already been committed. In this case, the police will protect the confidentiality of the information provided and if necessary, ensure the safety of the informant under the Law of Mongolia on Prevention of Crime (1997). However, the informer can be subject to criminal liability under the Criminal Code of Mongolia (2002) if they intentionally give false information to the police that another person has committed a crime.

Other than protection for those who are reporting crimes, a whistleblower does not have any legal protection under a dedicated law of Mongolia.

32.2 Is an English translation available?

No.

32.3 Is prior notification or approval required?

No.

32.4 Can notification or approval be filed online?

Not applicable.

32.5 Generally, how long does it take to get approval?

Not applicable.

32.6 Contact information for Data Protection Authority?

Not applicable.

32.7 What is the scope of reporting permitted?

There is no defined scope of reporting.

32.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No. Companies are free to design any whistleblower policy they deem appropriate. However, any whistleblowing program needs to be in compliance with the Personal Secrecy Law (1995), Organizational Secrecy Law (1995) and the State Secrecy Law (1995) in the case of a state organization. Failure to comply with these laws may result in criminal liability for disclosing confidential information, or for defamation. Therefore, even if a whistleblowing program is

implemented by a company, a whistleblower who discloses confidential information is not protected under the law as he/she is in breach of the prohibition on disclosure.

32.9 Are there limits to who can be subject of a report?

See above the answer to Question 32.8.

32.10 Is anonymous reporting permitted?

There is nothing specified in this regard under the law. Companies are free to determine their own policies on whether or not anonymous reporting is permitted.

32.11 Are there restrictions on the transfer of data in a whistleblowing program?

There is nothing specifically dealing with data sharing in relation to whistleblowing under the law. Even if the consent of the owner of the confidential information is obtained before the disclosure, the law does not contemplate whether the information can be disclosed.

If specified under a law, then information can be disclosed to the official of a government organization specified under that particular law.

32.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

As per above in the response to Question 32.11, the law does not stipulate a consent requirement for the transfer of data, and therefore there are no protections in place for the whistleblower, even if they do obtain consent.

32.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

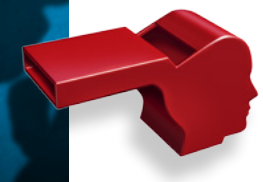
No.

32.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

No.

For more information, contact:

Name: Elisabeth Ellis
Firm: Minter Ellison
Address: Suite 612 Central Tower, Great Chinggis Khaan's Square 2, Sukhbaatar District – 8, Ulaanbaatar, Mongolia
Telephone: +976 7700 7780
Fax: +976 7700 7781
Email: elisabeth.ellis@minterellison.com
Website: www.minterellison.com



33. MONTENEGRO

33.1 Applicable law and/or data protection guidelines?

In Montenegro, whistleblowing is not regulated uniformly. Instead, provisions directly or indirectly regulating this area can be found in several laws and guidelines:

- Personal Data Protection Law;
- Labour Law;
- Law on Civil Servants and State Employees;
- Law on Free Access to Information;
- Law on Data Secrecy;
- Law on Protection of Undisclosed Data;
- Criminal Code; and
- Expert Instruction on Procedures for Reporting Criminal Offenses with Elements of Corruption and Protection of Persons Reporting these Offenses to the Police Administration.

33.2 Is an English translation available?

No.

33.3 Is prior notification or approval required?

Not applicable.

33.4 Can notification or approval be filed online?

Not applicable.

33.5 Generally, how long does it take to get approval?

Not applicable.

33.6 Contact information for Data Protection Authority?

Name:	Personal Data Protection Agency
Address:	Kralja Nikole 2, 81000 Podgorica, Montenegro
Telephone:	+382 20 634 894
Fax:	+382 20 634 883
Email:	azlp@t-com.me
Website:	www.azlp.me

33.7 What is the scope of reporting permitted?

There are certain restrictions imposed on reporting of information held by a public or government authority. Also, there are certain restrictions imposed on reporting of state-related information classified as confidential or secret (extending to some classified information of foreign countries and international organizations), which was made available or came into possession of a company or an individual.

33.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No.

33.9 Are there limits to who can be subject of a report?

No.

33.10 Is anonymous reporting permitted?

This matter is not explicitly regulated, but anonymous reporting would principally be permitted.

33.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes, general restrictions on transfer of data prescribed by the Personal Data Protection Law may also apply to data used in a whistleblowing program (e.g., written consent of employees, consent of the Personal Data Protection Agency).

33.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No, consent of employees is not required for a whistleblower program, but any creation of a special database for this purpose, including processing or transfer of personal data must be in accordance with requirements prescribed by the Personal Data Protection Law.

33.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

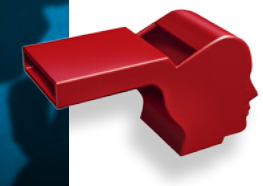
No.

33.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

No.

For more information, contact:

Name: Milica Popović
Firm: CMS Montenegro
Address: Bulevar Džordža Vašingtona 3/22, 81000 Podgorica, Montenegro
Telephone: +382 20 416 070 / +381 11 320 8900
Fax: +382 20 416 071
Email: milica.popovic@cms-rrh.com
Website: www.cms-rrh.com



34. MOZAMBIQUE

34.1 Applicable law and/or data protection guidelines?

Mozambique has no specific data protection laws in place.

However, despite not directly addressing the issue, the Constitution of Mozambique, the Mozambican Civil Code, the Labour Law (Law no. 23/2007, of August 1) and Law no. 34/2014, of December 31, provide for certain guidelines.

Article 71 of the Constitution establishes that the law shall provide for (i) a general protection of personal data in computer records, (ii) the requirements for access to databases and (iii) the terms of use by public and private authorities of these databases or computer media. However, these legal rules do not yet exist.

Article 80 of the Civil Code institutes the reserve on the intimacy of private life and Article 81 of the same law provides for the general regime of confidentiality of personal data, according to which the collection, processing and storage of personal data requires the explicit permission of the interested parties.

Regarding the employment relationship, Article 6 of the Labour Law provides for the protection of personal data, and, although specific regulations are not yet in force in what concerns the use of computer files and access to personal data related with job applicants or employees, it recognizes the employee's right, as a general rule, to confidentiality of correspondence of a personal nature made by means of electronic messages.

Finally, Law no. 34/2014, of December 31, regulates the exercise of public right to information and public democratic participation within the procedure and interaction between private entities or individuals and administrative and governmental bodies or entities. According to this law, the exercise of the public right to information and public democratic participation shall be made with respect to human dignity, namely, observing and respecting the right to honour, good name and reputation, as well as the right to defend the private life or data of the people concerned.

Consistent with this main principle, one of the most important rules introduced by Law no. 34/2014, of December 31, is that personal data or information regarding the privacy of people concerned, contained either on electronic or physical files held by such public entities, are classified as confidential and cannot be shared with any third or interested parties, unless in the case of express written consent of the people concerned or in case a court decision requires it. Any breach of these terms and conditions regarding the use of confidential information shall be punished with fines and may lead to criminal prosecution, on a case-by-case basis.

34.2 Is an English translation available?

An official English translation of the Constitution of Mozambique and of the Mozambican Civil Code is not available.

An English translation of Article 6 of the Labour Law (Law no. 23/2007, of August 1) is provided below:

"Article 6

(Protection of personal data)

1. Employers cannot, when appointing an employee or during the course of an employment contract, require the employee to provide information about his or her private life, except where, by virtue of the law or the practices of the occupation, the particular nature of the occupational activity so demands, and provided the reasons for the requirement are stated in writing beforehand.

2. The use of computer files and access relating to the personal data of a job applicant or employee shall be subject to specific legislation.

3. Personal data of an employee that has been obtained by an employer is subject to a duty of confidentiality, as is any other information of which dissemination would breach the employee's privacy. Neither shall be supplied to third parties without the consent of the employee unless legal reasons so require."

34.3 Is prior notification or approval required?

Not applicable.

34.4 Can notification or approval be filed online?

Not applicable.

34.5 Generally, how long does it take to get approval?

Not applicable.

34.6 Contact information for Data Protection Authority?

Not applicable.

34.7 What is the scope of reporting permitted?

Although there is no legal scope of reporting (please bear in mind our response to Question 34.1), the Labour Law establishes that the employing company can only disclose to third parties information on the employee's personal data in cases where the law, the practices of the occupation or the particular nature of the occupational activity so demands, and provided that the reasons for the requirement are stated in writing beforehand.

Nonetheless, access to personal computers of the employees by the company is not restricted by Mozambican law. Even if the employing company allows personal use, and certainly if that is prohibited, the employing company can access the computer to look at business-related information at any time. If, in doing so, it finds personal data, then that cannot be used and/or disclosed except by means of consent of the employee or a court ruling.

34.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

Not applicable.

34.9 Are there limits to who can be subject of a report?

Not applicable.

34.10 Is anonymous reporting permitted?

Not applicable.

34.11 Are there restrictions on the transfer of data in a whistleblowing program?

Please refer to the limitations described in our response to Question 34.7.

34.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

As a general rule, the consent of the employees is required for the transfer of their personal data. Please refer to the limitations described in our response to Question 34.7.

34.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

Not applicable.

34.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

Please refer to the limitations described in our response to Questions 34.1 and 34.7.

For more information, contact:

Name: Tomás Timbane
Firm: TTA Sociedade de Avogados
Address: Edifício Millennium Park, Torre A, Avenida Vladimir Lenine, nº 179, 6º Dtº, Maputo – Moçambique
Telephone: +258 843 141 820
Email: tomas.timbane@tta-advogados.com
Website: www.tta-advogados.com

Name: Miguel Spinola
Firm: PLMJ Sociedade de Advogados, RL
Address: Edifício Eurolex, Avenida da Liberdade, 224, 1250-148 Lisbon - Portugal
Telephone: +351 213 197 446
Mobile: +351 916 346 219 or +258 843 318 695
Fax: +351 21 319 74 00
Email: miguel.spinola@plmj.pt
Website: www.plmj.com

35. THE NETHERLANDS[23]

35.1 Applicable law and/or data protection guidelines?

The Netherlands currently has no specific whistleblower protection laws in place other than one relating to public servants employed by the government. The Safety Board for Government Integrity ("SBGI") was established by law and operates as an independent investigator of misbehaviour in the central government, police and defense sectors. The SBGI has been assigned the statutory task of handling abuse reported by a public servant whistleblower. The SBGI is entitled to independently investigate any misconduct in the event that a report is not handled properly by the relevant administrative body internally.

However, a bill is pending that will, when adopted, introduce an independent referral entity for whistleblowers, called the House for Whistleblowers (Huis voor Klokkenluiders). The House for Whistleblowers will be entitled to independently investigate reported abuse and misconduct, and advise and assist whistleblowers – in both the public and private sectors – and refer abuses to the competent authorities. The House for Whistleblowers will be bound to secrecy in respect of the identity of the whistleblower and the identity of the subject(s) of the alleged abuse by virtue of law. The bill furthermore introduces an obligation for companies to implement a policy on how they deal internally with the reporting of abuse and misconduct. The bill has to be adopted by the Dutch Senate, which is expected to happen in 2016.

Finally, the Dutch Corporate Governance Code Monitoring Committee presented the revised Dutch Corporate Governance Code (the "DCGC") on December 10, 2008. In 2004, this code was designated as a code of conduct to which listed companies should refer in their annual reports, where they should indicate to what extent they have complied with the principles and best-practice provisions ("the apply-or-explain principle"). The DCGC provides general rules in respect of whistleblowing programs in the private sector.

Whistleblower programs implemented by companies are assessed against the statutory requirements of the Dutch Personal Data Protection Act (Wet bescherming persoonsgegevens) and general principles of employment law, such as the concept of "good employership". In 2006, the Dutch Data Protection Authority ("Dutch DPA") issued an opinion on the data protection aspects of whistleblowing. Its position is that in order for the processing of personal data in the context of a whistleblowing program to be lawful, the processing should be necessary for the legitimate interest of the company and the fundamental rights and interests of data subjects should not prevail.

Several advisory bodies have rendered their opinions to the Dutch government. The Dutch DPA uses these opinions when assessing the compliance of data processing and/or transfer activities associated with whistleblower programs.

[23] The Netherlands are a member state of the European Union. If you are interested in the EU law requirements, please refer to the section on the European Union.

35.2 Is an English translation available?

The Dutch Corporate Governance Code is available in English at: http://commissiecorporategovernance.nl

An unofficial English language translation of the Dutch Personal Data Protection Act is available at: http://www.coe.int/t/dghl/standardsetting/dataprotection/national%20laws/NL_DP_LAW.pdf

35.3 Is prior notification or approval required?

A prior notification to the Dutch DPA is required with regard to the types of personal data (potentially) processed in the context of the whistleblower program. This notification does not entail approval of the actual program by the Dutch DPA.

35.4 Can notification or approval be filed online?

Yes, via the Dutch DPA's website (see below).

35.5 Generally, how long does it take to get approval?

Less than three months when personal data is only processed within the European Economic Area; three to six months in case of programs (where personal data is transferred to recipients outside of the European Economic Area).

35.6 Contact information for Data Protection Authority?

Name:	Dutch Data Protection Authority (College bescherming persoonsgegevens)
Address:	Juliana van Stolberglaan 4-10, 2595 CL Den Haag (The Hague)
Telephone:	+31 70 888 8 00
Website:	www.cbpweb.nl

35.7 What is the scope of reporting permitted?

The Dutch DPA stated that a whistleblowing hotline should be used only for reporting serious and substantial offenses. Financial reporting and corruption are most frequently mentioned as examples.

35.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No.

35.9 Are there limits to who can be subject of a report?

No. The legal framework does not provide specific restrictions. The seriousness of the reported abuse and its impact on the responsible organization is decisive, not the person or capacity of the subject of the report or the whistleblower.

35.10 Is anonymous reporting permitted?

Yes. However, the Dutch DPA stated that it prefers confidential reporting over anonymous reporting.

35.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes, the regular provisions regarding the (international) transfer of personal data apply.

35.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No.

35.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

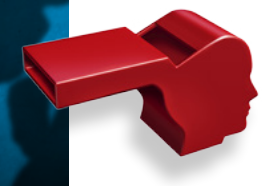
Yes. A whistleblower program qualifies as a complaints procedure under the Works Council Act (Wet op de ondernemingsraden). The Works Council has a right of consent with regard to decisions on the establishment, amendment or cancellation of such procedures. A decision to establish, amend or cancel a whistleblower program without the prior consent of the Works Council is void; that is, if the Works Council invokes the nullity of that decision in writing within one month from the time the decision comes to the knowledge of the Works Council.

35.14. Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

No.

For more information, contact:

Name: Hendrik Struik
Firm: CMS Netherlands
Address: Newtonlaan 203, 3584 BH Utrecht, The Netherlands
Telephone: +31 30 212 1726
Fax: +31 30 212 1157
Email: hendrik.struik@cms-dsb.com
Website: www.cms-dsb.com



36. NEW ZEALAND

36.1 Applicable law and/or data protection guidelines?

The Protected Disclosures Act 2000 was enacted to encourage people to report serious wrongdoing in their workplace by providing protection for employees who want to 'blow the whistle'. This applies to public and private sector workplaces, but is primarily concerned with public sector agencies.

Public sector agencies are required to establish internal procedures to handle whistleblowing complaints. There are also special rules on the procedures of intelligence and security agencies, and of certain organizations relating to international relations and intelligence and security.

Serious wrongdoing includes:

- Unlawful, corrupt or irregular use of public money or resources;
- Conduct that poses a serious risk to public health, safety, the environment or the maintenance of the law;
- Any criminal offense; or
- Gross negligence or mismanagement by public officials.

Additionally, other legislation contains protections for whistleblowers:

1. The Human Rights Act 1993 prevents any person from "victimizing" any other person on the grounds that the person has exercised their rights under the Protected Disclosure Act or intends to do so.
2. The Privacy Act 1993 contains implicit protections for whistleblowers. The Act provides that personal information can only be used and disclosed in connection with the purpose for which it was originally collected. However, non-compliance is permitted where such use or disclosure is necessary:
    a. To avoid prejudice to the maintenance of the law by any public sector agency (including the prevention, detection, investigation, prosecution and punishment of offenses); or
    b. To prevent or lessen a serious and imminent threat to public health or safety, or the life or health of any individual.

Accordingly, whistleblowers may not be in breach of the Privacy Act by disclosing personal information about others within their organization, provided such disclosure is within the parameters noted above.

36.2 Is an English translation available?

The primary language of the Protected Disclosures Act 2000, the Human Rights Act 1993 and the Privacy Act 1993 is English.

36.3 Is prior notification or approval required?

No, it is not necessary to seek approval from or notify any authority prior to setting up a whistleblower program.

However, if requested by the Ombudsman, a public sector organization must provide information about whether it has established and published internal procedures for receiving and dealing with information about serious wrongdoing, a copy of those procedures, and information about how those procedures operate.

36.4 Can notification or approval be filed online?

Not applicable.

We expect that any information requested by the Ombudsman can be provided in electronic form.

36.5 Generally, how long does it take to get approval?

Not applicable.

36.6 Contact information for Data Protection Authority?

Name:	Office of the Privacy Commissioner
Address:	PO Box 10-094, The Terrace, Wellington 6143, New Zealand
Telephone:	+64 0800 803 909
Email:	enquiries@privacy.org.nz
Website:	www.privacy.org.nz

36.7 What is the scope of reporting permitted?

Under the Protected Disclosures Act, disclosures will only be protected if:

- The information is about serious wrongdoing in or by the whistleblower's workplace;
- The whistleblower reasonably believes the information is true or likely to be true; and
- The whistleblower wants the serious wrongdoing to be investigated.

The Protected Disclosures Act also prescribes the person to whom the disclosure should be made, which varies depending on the internal procedures of the organization and the personnel implicated in the disclosure.

36.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

The Protected Disclosures Act protects disclosures of "employees" (defined under the Act as including former employees, homeworkers, contractors, people seconded to organizations and volunteers).

36.9 Are there limits as to who can be subject of a report?

No.

36.10 Is anonymous reporting permitted?

Yes, there is no requirement that employees disclose their name as part of their protected disclosure.

The Ombudsman recommends seeking specific advice about the circumstances in which anonymous disclosures can be made under the Protected Disclosures Act 2000.

36.11 Are there restrictions on the transfer of data in a whistleblowing program?

The underlying presumption is that protected disclosures must be kept confidential unless an exception applies.

The exceptions are if the whistleblower consents to the disclosure, or if disclosure is essential to:

- The effective investigation of the allegations;
- Prevent serious risk to public health or safety, or the environment; or
- Comply with the principles of natural justice.

An authority to whom a disclosure is made may also disclose that information to another appropriate authority if it considers that the information could be more suitably and conveniently investigated by that other authority.

We also note that the general restrictions on transfer of personal information in the Privacy Act 1993 will apply to whistleblowing programs.

36.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No.

36.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

No.

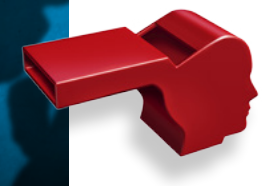
36.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

There are no specific computer or security requirements in relation to whistleblower programs. However, the Privacy Act 1993 provides that an agency holding personal information must ensure that the information is protected by such security safeguards as it is reasonable in the circumstances to take against loss, access, use, modification, disclosure or other misuse. In the whistleblowing context, this is likely to mean a higher threshold than usual, due to the sensitive nature of the personal information concerned.

The Privacy Act also requires that personal information is not kept for longer than is required for the purposes for which the information may lawfully be used. In the whistleblowing context, this is likely to mean that once any investigation has been concluded or the matter abandoned, all relevant personal information should be deleted.

For more information, contact:

Name: Richard Wells
Firm: Minter Ellison Rudd Watts Lawyers
Address: Lumley Centre, 88 Shortland Street, Auckland 1010, New Zealand
Telephone: +64 9 353 9908
Fax: +64 9 353 9701
Email: richard.wells@minterellison.co.nz
Website: www.minterellison.co.nz



37. NICARAGUA

37.1 Applicable law and/or data protection guidelines?

Nicaragua has no specific laws related to whistleblowing programs. However, there are labour laws and data protection laws that provide certain guidelines, although they do not directly address the issue.

For example, the Nicaraguan Labour Inspectors Law guarantees that employees who carry out any notification or complaints to the corresponding labour inspectors will remain anonymous.

37.2 Is an English translation available?

No, there are no official or non-official translations of the related legislation.

37.3 Is prior notification or approval required?

No, it is not necessary to notify any governmental institution or seek approval from any agency or authority to set up a whistleblowing program. However, in many cases, employers establish in their Internal Employee Guidelines (Reglamento Interno) certain dispositions regulating and providing steps and guidelines to be followed by employees for filing any complaint or denouncing any irregularities. These Internal Employee Guidelines must be approved by the Nicaraguan Labour Ministry.

Additionally, if the whistleblowing program includes the creation of a database with personal information of the employees (or information of any nature), it must comply with the requirements established in the Nicaraguan Data Protection Law regarding: i) procedure to collect, ii) storage of the data, iii) use of the data, iv) disclosure and v) assignment of data.

37.4 Can notification or approval be filed online?

Not applicable.

37.5 Generally, how long does it take to get approval?

Not applicable.

37.6 Contact information for Data Protection Authority?

As of this date, the Office for Protection of Personal Data ("DIPRODEC") is not yet operational. No contact information may be provided at this moment.

37.7 What is the scope of reporting permitted?

There is no limit to the scope permitted for reporting in whistleblowing programs in Nicaragua, as long as it does not concern facts about the employee that are beyond the scope of employment.

37.8 Are there limits as to who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No limitations may be identified in our legislation.

37.9 Are there limits as to who can be a subject of a report?

No limits may be identified in our legislation.

37.10 Is anonymous reporting permitted?

Yes. Anonymous reporting is allowed and usually implemented. In many circumstances, employers and governmental institutions such as the Ministry of Labour establish that the identity of employees who provide any information or complaint will be kept confidential.

However, the company in its investigation must obtain the information legally, guarantee the accused employee's right to be heard and the application of internal guidelines or procedures regarding any internal process.

37.11 Are there restrictions on the transfer of data in a whistleblowing program?

There are no specific dispositions regarding the transfer of data for a whistleblowing program. However, in general, personal data may only be assigned or transferred, subject to the prior consent of the data owner. The data owner has the right to know the purpose of the assignment and the identification of the assignee. The authorization or consent to assign may be revoked by the owner in writing.

Consent will not be required if: (a) there is a specific law authorizing it, (b) the transfer is made among governmental institutions and within their attributions, (c) for any public interest reason such as public health or national interest, or (d) a dissociation process has been applied to the data. Data transfer must comply with minimum security measures and adequate protection. Likewise, data transfer must be notified to the Office for Protection of Personal Data ("DIPRODEC"), which is not yet operational.

37.12 Is the consent of employees required for either a whistleblowing program or for the transfer of data in a whistleblowing program?

There is no consent requirement for a whistleblowing program; however, in accordance with the response to the previous question, the Nicaraguan Data Protection Law provides that personal data collection and treatment must have prior consent from the individual.

Consent must be granted in writing or by any other suitable means, physical or electronic. Consent may be revoked, without retroactive effects, by any means permitted by law.

Prior authorization will not be required in the following cases: (a) for obtaining data from sources with unrestricted public access and for obtaining data from lists that only include

the name, identification number, and date of birth; (b) when there is a judicial order; (c) when the personal data is subject to a previous dissociation process; and (d) the data is required to comply with a juridical relationship between the data owner and the data holder (such as an employment relationship).

37.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

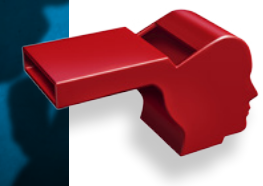
No. In accordance with Nicaraguan legislation, there is no need for consultation with a Works Council or any union or other employee representative group for the implementation of a whistleblowing program.

37.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

The Nicaraguan Data Protection Law states that the creators of data files must take such technical and organizational measures necessary to guarantee the security and confidentiality of personal data, in order to avoid its alteration, loss, unauthorized consultation or treatment, and which allow for the detection of any intentional or unintentional distortion of such information.

For more information, contact:

Name: Roberto Argüello
Firm: Arias & Muñoz
Address: Pista Jean Paul Genie, Edificio Escala, 3er piso, Managua, Nicaragua
Telephone: +505 2298 1360
Email: roberto.arguello@ariaslaw.com
Website: www.ariaslaw.com



38. NORWAY

38.1 Applicable law and/or data protection guidelines?

In Norway, we have both specific whistleblower legislation and data protection guidelines. In 2007, Norway amended its Working Environment Act (the "WEA") to add provisions for the protection of employees who report "censurable conditions" in the organization. These provisions give the employees the right to report, and specifically prohibit retaliation against an employee who makes use of this right. Retaliation means any kind of unfavorable treatment that can be seen as a reaction to or a consequence of the report.

Furthermore, the employer is obligated to establish policies for internal notification or implement other measures that enable the employees to make use of the right. Such policies should, as a minimum, explain when the right to notify can be used, to whom the notification shall be given, which procedures should be followed and how the report will be handled by the employer.

There are no specific requirements in relation to how the program has to be set up, and the company may use both hotlines and websites, and also outsource the operation of the whistleblowing procedures to a data processor.

Additionally, the Personal Data Act and the Personal Data Regulations (together, the "DPL") apply to the processing of personal data that is reported through and collected in whistleblowing programs.

38.2 Is an English translation available?

Yes. The following translations are available:

Working Environment Act:
www.arbeidstilsynet.no/binfil/download2.php?tid=92156

The Personal Data Act:
www.datatilsynet.no/English/Regulations/Personal-Data-Act-/

The Personal Data Regulations:
www.datatilsynet.no/English/Regulations/Personal-Data-Regulations

The DPA guidelines are not available in English.

38.3 Is prior notification or approval required?

Yes. However, usually a license from the DPA is required because information relating to criminal offenses is considered sensitive data. However, if a whistleblowing program is only available for employees, a notification to the DPA is sufficient.

If the whistleblowing program will be used by others, such as consultants or customers, a license from the DPA is required.

38.4 Can notification or approval be filed online?

Yes. A notification can be filed online but a license application must be mailed to the DPA.

38.5 Generally, how long does it take to get approval?

A notification has to be filed no later than 30 days prior to commencement of processing. The notification is not subject to the DPA's approval as it only serves as a notice regarding the planned processing of personal data.

Obtaining a license takes approximately 8-12 weeks, provided that all documentation requirements are fulfilled.

38.6 Contact information for Data Protection Authority?

Name:	The Norwegian Data Protection Authority
Address:	P.O. Box 8177 Dep, N-0034, Oslo, Norway
Telephone:	+47 22 39 69 00
Email:	postkasse@datatilsynet.no
Website:	www.datatilsynet.no

38.7 What is the scope of reporting permitted?

The right to notify – and the following protection against retaliation in the Working Environment Act – is limited to reports about "censurable conditions". The term "censurable conditions" means situations that are of a certain severity, inter alia, legal offenses such as corruption and other types of financial crime, breaches of the company's ethic codes, hazardous working conditions, discrimination and harassment.

Circumstances that an employee considers to be censurable based on his/her own political or ethical convictions are, however, not necessarily "censurable conditions". This is due to the fact that censurable conditions should have a certain general interest. Furthermore, whistleblowing within the meaning of the WEA does not include communication of personal ideas and experiences, feelings and thoughts that are not of general interest. Neither is it considered as whistleblowing to notify situations where an employee disagrees with the employer's decisions, unless the employer's decision may result in an illegal action or an action that is in conflict with a general ethical standard.

However, there are no formal restrictions that prevent the employer allowing the employees to use the system/program to report other internal matters.

38.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No. The rules in the Working Environment Act apply to all employees in both the private and public sectors and comprise both internal notifications and reports to e.g., the media, supervisory authorities, etc.

It has been discussed if also temporary personnel, who are employed by a temporary staff recruitment agency, enjoy the same protection as the company's ordinary employees when they blow the whistle about conditions in the company in which they are hired to work. A direct interpretation of the law would exclude such personnel from the Working Environment Act's protection against retaliation from the hiring company. However, the rationale behind the legal protection of whistleblowers can be used as an argument for considering such personnel as covered by the whistleblower provisions. This question is, however, yet to be answered.

As there are no legal limits on who can make a report through a whistleblowing program, it may also be available for external parties such as suppliers and contractors as well as employees.

38.9 Are there limits to who can be subject of a report?

No.

38.10 Is anonymous reporting permitted?

Yes. Anonymous reporting is permitted and many whistleblowers prefer to stay anonymous. Usually, companies have special rules concerning this.

38.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes. The DPL not only sets out conditions that must be fulfilled in order to legally process personal data, but also includes restrictions on the possibility to transfer the personal data, and thus also the reports, to countries outside the EU.

Within the EU, the possibility of transferring the personal data is unlimited, as it is based on a presumption that the transfer is made to a state that ensures an adequate level of protection of the data/information.

In relation to transfers outside the EU, data may be transferred to countries with the same safety and data protection standards as the EU. The level of protection is satisfactory if:

- The country is designated by the European Commission as having adequate protection;
- The EU Standard Contractual Clauses for transfer are used. This requires a notification to the DPA in advance;
- The data importer and data exporter is part of the same corporation and have decided on Binding Corporate Rules.

Transfer of data to countries that do not ensure an adequate level of protection might also take place if the data subject has consented to the transfer, and if the transfer is necessary in order to establish, exercise or defend a legal claim.

38.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No.

38.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

No. There is an obligation for the employer to establish routines for internal notification or implement other measures that enable the employees to make use of the right to whistle-blow. Consent/consultation is therefore not a requirement. However, it may be wise to discuss the potential whistleblowing with a Works Council, union or other employee representative before it is implemented as this may increase its credibility.

38.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

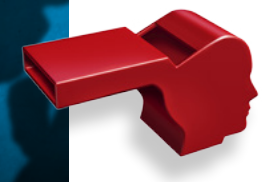
Yes. The data controller (and data processor, if any) shall by means of planned, systematic measures ensure satisfactory data security with regard to confidentiality, integrity and accessibility in connection with the processing of personal data.

The controller and processor therefore have to implement both technical, physical, organizational and personnel security measures in order to ensure satisfactory data security. The purpose is to prevent unauthorized/unlawful processing and accidental loss, damage and destruction of personal data.

Personal data must be deleted when no longer necessary to carry out the purpose of the processing. According to administrative practices from the DPA, personal data in a whistleblowing system must be deleted two months after closing the investigation unless other purposes legitimize longer storage.

For more information, contact:

Name: Kaare Risung or Trond Stang
Firm: Advokatfirmaet Schjødt AS
Address: Ruseløkkveien 14, P.O. Box 2444 Solli, NO-0201 Oslo, Norway
Telephone: +47 23 01 18 00
Fax: +47 22 83 1712
Email: kmr@schjodt.no or trst@schjodt.no
Website: www.schjodt.no



39. PANAMA

39.1 Applicable law and/or data protection guidelines?

Panama does not have specific legislation governing whistleblowing programs.

However, Panama's Constitution guarantees various rights to privacy (Articles 42 to 44) and it has a number of laws and regulations governing data protection in various sectors including public administration and services, health information, financial services, telecommunications and others, which may have a bearing on the set-up and operation of a whistleblowing program.

39.2 Is an English translation available?

Not applicable.

39.3 Is prior notification or approval required?

Not applicable.

39.4 Can notification or approval be filed online?

Not applicable.

39.5 Generally, how long does it take to get approval?

Not applicable.

39.6 Contact information for Data Protection Authority?

Panama does not have a Data Protection Authority.

39.7 What is the scope of reporting permitted?

Since Panama does not have a specific regulation on whistleblowing programs, it will depend on the situation and a case-by-case review of applicable regulation.

39.8 Are there limits as to who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No.

39.9 Are there limits as to who can be a subject of a report?

No.

39.10 Is anonymous reporting permitted?

Since Panama does not have a specific regulation on whistleblowing programs, it will depend on the situation and a case-by-case review of applicable regulation.

39.11 Are there restrictions on the transfer of data in a whistleblowing program?

It depends on the situation and a case-by-case review of the applicable regulation.

39.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

Since Panama does not have a specific regulation on whistleblowing programs, it will depend on the situation and a case-by-case review of applicable regulation.

39.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

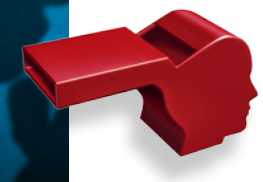
Since Panama does not have a specific regulation on whistleblowing programs, it will depend on the situation and a case-by-case review of applicable regulation.

39.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

Since Panama does not have a specific regulation on whistleblowing programs, it will depend on the situation or a case-by case-review of applicable regulation.

For more information, contact:

Name: Siaska Lorenzo, Partner
Firm: Arias & Muñoz
Address: Torre Global, Piso 23, Oficina 2305, Calle 50, Panama City, Panama
Telephone: +507 282 1400
Fax: +507 282 1435
Email: siaska.lorenzo@ariaslaw.com
Website: www.ariaslaw.com



40. PERU

40.1 Applicable law and/or data protection guidelines?

There are no specific regulations concerning whistleblowing in Peru. Nevertheless, Law No. 29733, Personal Data Law, its regulations, approved by Supreme Decree N° 003-2013-JUS (the "Personal Data Regulation") may be applicable.

40.2 Is an English translation available?

No

40.3 Is prior notification or approval required?

The implementation of a whistleblowing program is not subject to any notification or approval.

Nevertheless, if the information related to the whistleblower is related to an "individual", it will be regarded as "personal data". In that regard, according to the Personal Data Regulation, the processing of personal data (including its collection) is subject to informed consent requirements, as a general rule.

In particular, consent for the processing of "sensitive data", which refers to information on the racial or ethnical origin of a person, financial income, political opinions or convictions, union membership, health-related information and biometric data among other types of information, must be obtained in writing.

Additionally, if the whistleblowing program handles personal data stored in a database, the company must notify the creation of the database and register it before the Data Protection Authority prior to commencing processing of the data.

40.4 Can notification or approval be filed online?

As mentioned above, the implementation of the whistleblowing program is not subject to any notification or approval.

Regarding personal data treatment, consent of the personal data holder may be obtained through electronic means. However, if the whistleblowing program treats "sensitive data", consent must be obtained in writing.

40.5 Generally, how long does it take to get approval?

Not applicable.

40.6 Contact information for data protection authority

Name: Autoridad Nacional de Protección de Datos Personales
Address: Calle Scipión Llona Nº 350, Miraflores, Lima 18, Peru
Telephone: +511 204 8020 ext. 1030
Email: apdp@minjus.gob.pe
Website: www.minjus.gob.pe/proteccion-de-datos-personales

40.7 What is the scope of reporting permitted?

There is no limit to the scope permitted for reporting in whistleblowing programs.

Notwithstanding this, despite not having regulations regarding the access to an employee's personal information (e-mail accounts, cell phones provided by the company, etc.), a Constitutional Court ruling (contained in Court File N° 1058-2004-AA/TC) declares that employers require the employee's prior consent to access this personal information.

40.8 Are there limits as to who can make a report under a whistleblowing program?

No.

40.9 Are there limits as to who can be a subject of a report?

No.

40.10 Is anonymous reporting permitted?

Yes.

40.11 Are there restrictions on the transfer of data in a whistleblowing program?

If personal data is treated through the whistleblowing program and transferred abroad, rules on cross-border flows of personal data will apply.

Cross-border transfer of personal data is allowed to countries that maintain adequate levels of protection as prescribed by Peruvian regulation. In cases where the recipient country does not have an adequate level of protection, the agent responsible for the cross-border transfer must ensure that the processing of the personal data is carried out as provided by Peruvian regulation.

The controller will be required to notify the Peruvian Personal Data Protection Authority of the cross-border transfer of personal data.

40.12 Is the consent of employees required for either a whistleblowing program or for the transfer of data in a whistleblowing program?

There is no requirement for the consent of employees for the implementation of a whistleblowing program. Nevertheless, as a general rule, data subjects (the employees) must be informed of any personal data processing and grant their consent.

40.13 Is the consent of, or consultation with, a work council, union or other employee representative group required?

No.

40.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

No. However, if personal data is treated through the whistleblowing program, the company must comply with the security measures established in the Personal Data Regulation.

For more information, contact:

Name: Carlos A. Patron or Giancarlo Baella
Firm: Payet Rey Cauvi Perez Abogados
Address: Av. Victor Andres Belaunde 147, Centro Empresarial Real, Torre Real Tres Piso 12, San Isidro, Lima 27, Perú
Telephone: +511 612 3202
Fax: +511 222 1573
Email: cap@prc.com.pe or gbp@prc.com.pe
Website: www.prc.com.pe

41. PHILIPPINES

41.1 Applicable law and/or whistleblower protection guidelines?

The Philippines has whistleblower protection laws in place to encourage disclosures of wrongdoing both in the public and private sectors. While there is no whistleblower protection code, the following are some of the laws that provide for whistleblowing:

- Presidential Decree No. 442 or the Labour Code of the Philippines provides that the act of an employer of dismissing, discharging or otherwise causing prejudice or discriminating against an employee for having given testimony in relation to a violation of the law shall be construed as an unfair labour practice;
- Republic Act No. 6981 or the Witness Protection, Security and Benefit Act provides protection, security and benefits to witnesses of criminal acts;
- Presidential Decree No. 749 grants immunity from prosecution to givers of bribes and other gifts in bribery and other graft cases against public officers;
- Republic Act No. 6770 or the Ombudsman Act of 1989 empowers the Ombudsman to grant immunity from criminal prosecution to any person whose testimony or whose possession and production of documents or other evidence may be necessary to determine the truth in any hearing, inquiry or proceeding being conducted by the Ombudsman;
- Commonwealth Act No. 108 or the Anti-Dummy Law grants a reward to an informer who furnishes to the government original information leading to conviction for a violation of this law, and immunity to an "informer-dummy" who voluntarily reports a violation of this law and assists in the prosecution of a case; and
- Republic Act No. 10667 or the Philippine Competition Act mandates the Philippine Competition Commission to develop a leniency program for the grant of benefits such as immunity from suit which would otherwise be filed against, and a reduction of a fine which would otherwise be imposed on, a participant in an anti-competitive agreement in exchange for the voluntary disclosure of information regarding such an agreement, subject to criteria specified in the law. To date, the Philippine Competition Commission has yet to formulate a leniency program.

41.2 Is an English translation available?

Yes. English is one of the official languages of the Philippines. Laws and regulations are promulgated in English.

41.3 Is prior notification or approval required?

No prior notification to or approval by a government agency or entity is required for a private corporation to establish a whistleblowing program.

Admission to the Witness Protection Program under the Witness Protection, Security and Benefit Act, requires the approval of the Philippine Department of Justice ("DOJ").

41.4 Can notification or approval be filed online?

Not applicable with respect to the establishment by a private corporation of a whistleblowing program.

41.5 Generally, how long does it take to get approval?

Not applicable with respect to the establishment by a private corporation of a whistleblowing program.

41.6 Contact information for Data Protection Authority?

The Data Privacy Act of 2012 created the National Privacy Commission under the Office of the President. However, it has yet to be constituted.

With respect to the Witness Protection Program pursuant to the Witness Protection, Security and Benefit Act, the DOJ's contact details are as follows:

Name:	Department of Justice
Address:	Padre Faura Street, Ermita, Manila 1000, Republic of the Philippines
Telephone:	+632 523 8481
Email:	communications@doj.gov.ph
Website:	www.doj.gov.ph

41.7 What is the scope of reporting permitted?

Subject to specific requirements under applicable law, a report can generally cover any violation of the relevant law.

41.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

The relevant Philippine laws generally do not provide limitations on who can make a report of a violation, assuming that the person giving a report is not bound to keep such information confidential, or such information is not privileged. There should, however, be compliance with the requirements under the applicable law in order to avail the whistleblower of protection and benefits granted by that law.

41.9 Are there limits on who can be a subject of a report?

The limits on who can be a subject of a report depend on the applicable law.

41.10 Is anonymous reporting permitted?

Yes.

41.11 Are there restrictions on the transfer of data in a whistleblowing program?

The Data Privacy Act of 2012 provides restrictions on the disclosure and processing of personal information. However, this law, under certain circumstances, allows the processing of personal information when it is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to the government.

41.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

The consent of employees is not required for a private corporation to create a whistleblowing program.

Regarding the transfer of personal information, the Data Privacy Act of 2012 generally requires the consent of the data subject, but the law provides for certain exemptions.

41.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

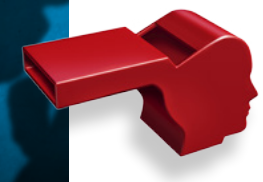
The consent of a union or an employee representative group is not required for a private corporation to create a whistleblowing program, subject to stipulations in any collective bargaining agreement or other agreement between the employer corporation and its employees.

41.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

With respect to personal information, the Data Privacy Act of 2012 provides that personal information can be retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained, or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by other applicable law.

For more information, contact:

Name	Rolando V. Medalla, Jr. or Hiyasmin H. Lapitan or Azyleah V. Ignacio or Patricia A. Madarang
Firm:	SyCip Salazar Hernandez & Gatmaitan
Address:	SyCipLaw Center, 105 Paseo de Roxas, Makati City 1226, The Philippines
Telephone:	+63 2 982 3500 or +63 2 982 3600, or +63 2 982 3700
Fax:	+63 2 817 3145 or +63 2 817 3896
Email:	rvmedalla@syciplaw.com or hhlapitan@syciplaw.com or avignacio@syciplaw.com or pamadarang@syciplaw.com
Website:	www.syciplaw.com



42. POLAND[24]

42.1 Applicable law and/or data protection guidelines?

Currently in Poland, there are neither specific laws concerning whistleblowing programs nor any relevant guidelines provided by the Data Protection Authority ("DPA"). The DPA, however, does not remain ignorant of the issue and emphasizes the importance of whistleblowing programs. The DPA actively participates in public debate involving representatives of the legal profession, employers and the government. The scope of the debate covers not only problems connected with whistleblowing itself, but also future challenges related to the possible implementation of relevant Polish regulations.

Consequently, the general guideline in this area is Working Paper No. 117 of the Article 29 Data Protection Working Party ("the 29 WP Opinion") on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, bribery, banking or financial crimes. A second document that may constitute supplementary guidelines is Recommendation CM/Rec (2014)7 of the Committee of Ministers of the Council of Europe adopted for the protection of whistleblowers ("CoE Recommendation") supplementing Resolution 1729 (2010) of the Council of Europe and directed towards all member states.

Currently, Polish legal doctrine seeks a legal basis for whistleblowing programs in the provisions of Polish labour law, which oblige employees to protect the general welfare and property rights of the workplace and to comply with the principles of social interaction.

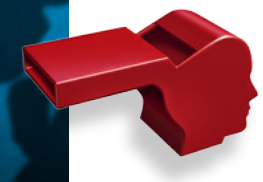
42.2 Is an English translation available?

No. However, the Act on Personal Data Protection ("PDP") has been translated to English and is available on the official website of the DPA at:

www.giodo.gov.pl/143/j/en/

42.3 Is prior notification or approval required?

The law does not require any kind of notification or approval to launch a whistleblowing program in a workplace. There is also no obligation to register the personal data information system containing the data of employees or service providers involved in the whistleblowing procedure by a given data controller. In such cases, the employer may benefit from a general statutory exemption from obligations related to registering data on the personal data system. However, if the personal data system contains the personal data of third parties (vendors, clients, employees of third parties, including affiliates), it is subject to regular registration obligations, i.e., it should be registered with the DPA or in the register managed by a Data



[24] Poland is a member state of the European Union. If you are interested in the EU law requirements, please refer to the section on the European Union.

Protection Officer (if the data controller has appointed a Data Protection Officer). It is then necessary to file the relevant application before the processing starts.

42.4 Can notification or approval be filed online?

Not applicable. However, if the data controller is obliged to register a personal-data filling system related to a whistleblowing program, it may be registered on the DPA's official website: https://egiodo.giodo.gov.pl/personal_data_register.dhtml or in the register managed by a Data Protection Officer (if the data controller has appointed one).

42.5 Generally, how long does it take to get approval?

Not applicable.

42.6 Contact information for Data Protection Authority?

Name:	The Bureau of the Inspector General for Personal Data Protection (Biuro Generalnego Inspektora Ochrony Danych Osobowych)
Address:	ul. Stawki 2, 00-193 Warszawa, Poland
Telephone:	+48 22 860 7086
Fax:	+48 22 860 7086
Email:	kancelaria@giodo.gov.pl
Website:	www.giodo.gov.pl

42.7 What is the scope of reporting permitted?

Due to the lack of a legal definition of whistleblowing in Polish law, the scope of actions that might be reported by the whistleblower should be broad but relevant, and not excessive in relation to the purposes for which the data are collected. Reported actions may concern serious matters having a significant influence on the functioning of the company or life or health of involved persons. The spectrum of such information reported in the course of internal whistleblowing programs should be defined and limited accordingly, and include the following: corruption or fraud; illegal, fraudulent or risky activity that is detrimental to the common good; intended or committed offenses; failure to fulfill obligations stipulated in law; abuses of power by judicial authorities; serious risk posed to public health, safety and natural environment; unauthorized use of public funding; maladministration; abuse of competence; conflict of interests; and manners of conduct threatening or causing damage to the employer's assets.

42.8 Are there limits as to who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

There are no legal limits as to the persons who are authorized to report as whistleblowers. This issue should be approached individually by a given company, e.g., in its internal regulations such as a whistleblowing policy. The 29 WP Opinion provides that specific details should depend on the circumstances of each individual case but simultaneously suggests considering the introduction of restrictions in this regard, in particular in the light of the seriousness of

alleged crimes. Still, in no way do the provisions exclude the possibility to grant such a right to every employee.

According to Polish jurisprudence, a right to report under a whistleblowing scheme should be granted to every employee regardless of the legal grounds of their employment. The CoE Recommendation implies that the right has a universal dimension. The employee's general obligation to protect and exercise care at the workplace as provided in the Labour Code is understood by some authors as entailing an obligation to act as a whistleblower when necessary, e.g., if there is a danger to the company's assets or possible damage the employer might incur.

42.9 Are there limits as to who can be a subject of a report?

No, but this matter is a subject of ongoing debate. In general, there are no legal limits imposed in this area. The 29 WP Opinion suggests that the relevant decision should be taken by the data administrators individually. Reducing the scope of persons subject to reporting is worth considering, depending on the circumstances of each particular case, especially considering the seriousness of the alleged crimes.

It is advisable that internal regulations on whistleblowing programs specify relevant limits and detailed categories of persons whose misconduct may be reported.

42.10 Is anonymous reporting permitted?

Polish law does not regulate this issue. However, based on the 29 WP Opinion anonymous reports should be an exception, not the rule. Anonymity should not be encouraged with respect to reporting various irregularities. Anonymous reports do not ensure the fair collection of the personal data and do not prevent a wide range of problems connected with the workplace atmosphere, mutual suspicions, an increasing number of malevolent reports and difficulties in conducting inspections. For this reason, the CoE Recommendation attaches special emphasis on making personally identified reports a main principle in whistleblowing. Obviously, this does not entail that the confidentiality of a whistleblower's personal data might be compromised.

42.11 Are there restrictions on the transfer of data in a whistleblowing program?

The general rules applicable to international transfers of personal data apply. This means that the transfers are allowed only if the destination country belongs to the EEA or provides the same or higher level of data protection as Poland. Alternatively, such transfers are allowed if the transfer is performed under an agreement made between the transferor and the transferee, and that the agreement conforms to the Standard Contractual Clauses adopted by the EU Commission. Otherwise, it is obligatory to obtain prior permission from the DPA. However, if both the transferor and the transferee belong to the same group of entities that have adopted Binding Corporate Rules, which have been approved by a DPA in another EEA state, the Polish DPA might simply acknowledge such approval.

42.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

In the DPA's view, if an employer transfers employees' personal data to another entity (controller or processor) within the whistleblowing program, this does not require employees' consent, as such transfer is based on the legitimate interest of the data controller. However, the employer should always attempt to balance the legitimate interests of personal data processing with the rights and freedoms of data subjects, paying attention to proportionality and the subsidiary nature of measures applied in whistleblowing programs. These programs should provide data subjects with an additional reporting mechanism regarding internal misconduct, including the seriousness of alleged offenses as well as their consequences.

However, the employees need to be informed about the introduction of a whistleblowing program, its purpose and function, as well as related internal regulations or policies, and about all rights provided in the data protection law (e.g., right to access, right to request rectification, blocking or deletion of any outdated or incorrect data, etc.).

42.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

No, under Polish labour law neither the whistleblower program nor the transfer of employees' personal data requires consultation or cooperation with the Works Council, nor with trade unions, nor any other employees' representative bodies. However, the internal policies of a given employer or agreements entered into with the abovementioned bodies might contain different provisions as to this issue. In our experience, it is extremely rare that agreements between these entities regulate personal data transfers or a whistleblower program. It should be also noted that there are no legal provisions or judgments of the Polish Supreme Court directly addressing the whistleblower issue under Polish labour law.

42.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

No. However, pursuant to the WP 29 Opinion, the principle of proportionality requires that the personal data be collected and processed honestly with respect to the purpose for which it has been collected. The data should be deleted within two months of the date the investigation reaches its conclusion, unless legal or disciplinary proceedings or archiving rules require a longer storage period.

Processing of personal data collected in the course of a whistleblowing program is subject to general security requirements. A data controller shall take technical and organizational measures to ensure the protection of the personal data it processes. Such measures must

accommodate relevant risks and categories of the data to be protected. In particular, the controller shall secure the data against disclosure to unauthorized persons, removal by an unauthorized person, processing in violation of the provisions of the PDP, or other instances of unauthorized modification, loss, damage or destruction. The above measures and safeguards should be described in the applicable internal policies.

The details of the requirements that a data controller must meet were specified in the Regulation of April 29, 2004, issued by the Minister of Internal Affairs and Administration on the documentation of the personal data processing and technical and organizational conditions, which should be fulfilled by devices and computer systems used for personal data processing.

For more information, contact:

Name: Agata Szeliga or Katarzyna Paziewska
Firm: Sołtysiński Kawecki & Szlęzak
Address: ul. Jasna 26, 00-054 Warszawa, Poland
Telephone: +48 22 608 7006 or +48 22 608 7190
Fax: +48 22 608 7070
Email: agata.szeliga@skslegal.pl or katarzyna.paziewska@skslegal.pl
Website: www.skslegal.pl

43. PORTUGAL[25]

43.1 Applicable law and/or data protection guidelines?

Portugal has no specific whistleblower protection laws in place. The implementation of a whistleblower program is subject to the Portuguese Data Protection Act.

The Portuguese Data Protection Authority ("DPA") has issued Resolution No. 765/2009 under which it settled applicable principles to whistleblower programs.

43.2 Is an English translation available?

Yes, a translation is available at:

www.cnpd.pt/english/bin/legislation/Law6798EN.HTM

Resolution No. 765/2009 of the DPA is only available in Portuguese.

43.3 Is prior notification or approval required?

Yes, an approval from the DPA is required.

43.4 Can notification or approval be filed online?

Yes, the request for approval can only be filed online and it has to be made in the Portuguese language.

43.5 Generally, how long does it take to get approval?

Usually, approval takes more than six months. However, the DPA has made a serious effort to reduce its response time and it has been possible to obtain a decision within six months.

43.6 Contact information for Data Protection Authority?

Name:	Comissão Nacional de Protecção de Dados (CNPD)
Address:	Rua de São Bento, 148 3º, 1200-821, Lisboa, Portugal
Telephone:	+351 21 392 8400
Email:	geral@cnpd.pt
Website:	www.cnpd.pt

43.7 What is the scope of reporting permitted?

Whistleblowers are only allowed to report on bookkeeping, internal accounting controls, auditing matters, corruption, banking and financial crimes.

[25] Portugal is a member state of the European Union. If you are interested in the EU law requirements, please refer to the section on the European Union.

43.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

Yes. Only employees are allowed to report.

43.9 Are there limits on who can be a subject of a report?

Yes. Information collected and processed under the whistleblower program must only concern individuals who are involved in management decisions in bookkeeping, internal accounting controls, auditing matters, corruption, banking and financial crimes (i.e., managerial positions).

Therefore, the whistleblower program cannot be used for the investigation of incriminating reports regarding personnel who have no involvement whatsoever in the company's management decisions.

Reports on employers of other companies or external suppliers are not admissible.

43.10 Is anonymous reporting permitted?

No.

43.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes. A transfer to countries outside the EU can only take place if:

(a) The data subject has provided unambiguous consent to the data transfer; or

(b) Standard Contractual Clauses for the transfer of personal data are used as approved by the European Commission; or

(c) The DPA previously approved clauses regulating the data transfer different from those approved by the European Commission (the evaluation of such clauses by the DPA may delay the approval of the whistleblower program).

43.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No. But if consent is not obtained, the data transfer can take place if the DPA accepts that the data transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims. When transfer is made to a data processor in a country that ensures an adequate level of protection, the DPA authorizes the transfer (e.g., conclusion of the Standard Contractual Clauses as approved by the European Commission).

43.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

No. However, it is advisable to notify the Works Council in advance.

43.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

Yes. Resolution No. 765/2009 of the DPA indicates the following as the minimum acceptable for data security:

(a) The computerized system should be organized in a way as to allow data access only upon user identification and individual passwords or any other authentication mechanism, to be renewed from time to time;

(b) All data accesses should be recorded (logged) and regularly monitored;

(c) Access to servers should be restricted to authorized personnel only (physical and computerized access); and

(d) Back-up copies are required and should be accessed only by the system's administrator.

With regard to data deletions, the following should be observed:

(a) Data contained in a report should be immediately eliminated if found inaccurate or useless;

(b) In cases where no disciplinary or judicial procedures will take place, evidence-based data will be destroyed six months after examination has ended; and

(c) In cases where disciplinary or judicial procedures take place, data shall be kept until these procedures are finished.

For more information, contact:

Name: Daniel Reis or Marta Costa
Firm: PLMJ – Sociedade de Advogados, RL
Address: Lisboa Av. da Liberdade, 224, Edifício Eurolex, 1250-148 Lisboa, Portugal
Telephone: +351 21 319 7300 or direct dial +351 21 319 7313
Fax: 351 21 319 7400
Email: daniel.reis@plmj.pt or marta.costa@plmj.pt
Website: www.plmj.pt

44. RUSSIA

44.1 Applicable law and/or data protection guidelines?

Russia has no specific whistleblower protection laws in place.

The whistleblower program shall be implemented in compliance with the Federal Law No. 152-FZ dated July 27, 2006, On Personal Data (the "Personal Data Law") and the Labour Code of the Russian Federation.

44.2 Is an English translation available?

Yes. An unofficial translation of the Personal Data Law (without the recent amendments) can be found at the personal data portal of the Russia Data Protection Authority: http://pd.rkn.gov.ru/authority/p146/p164.

44.3 Is prior notification or approval required?

No. The notification of the Data Protection Authority is not required if, as part of the whistleblowing program, the personal data is processed solely in connection with labour relations (further to an exemption provided for in the Personal Data Law).

However, any excessive operations with the employees' personal data may go beyond this framework and, therefore, the "general" notification on processing of personal data will be required by statute. The same applies to processing of other subjects' (different from the employees) personal data out of scope of contractual relations with the data subject.

As a consequence, if not only the information on the employees is collected within the whistleblowing program, and the purpose of data collection is not linked to labour relations (or any other contractual relations) the notification of the Russian Data Protection Authority is necessary.

44.4 Can notification or approval be filed online?

Yes. If necessary, the general notification on processing of personal data can be filed online.

44.5 Generally, how long does it take to get approval?

Where applicable, the registration is made by the Data Protection Authority ("Roskomnadzor") within 30 days from the receipt of the notification. This term has been reduced by the internal regulations of the Data Protection Authority to 15 days.

44.6 Contact information for Data Protection Authority?

Name:	The Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (Roskomnadzor)
Address:	Kitaygorodsky proezd, 7, building 2, Moscow, 109074, Russia
Telephone:	+7 495 987 6800
Email:	rsoc_in@rkn.gov.ru
Website:	rkn.gov.ru

44.7 What is the scope of reporting permitted?

From a labour law perspective, it is advisable to draft a comprehensive whistleblowing policy to govern the specific aspects of the whistleblowing program and permitted scope of reporting so that the reported information may be used as a ground for disciplinary actions.

The personal data should relate to the performance of working duties by employees and their behaviour at work and should not contain details of employees' private life (the restriction needs to be stipulated in the local whistleblowing policy), otherwise whistleblowers may be held liable for an unauthorized disclosure of private life secrets.

To this end, it is recommended to limit the scope of the whistleblowing program only to the reports on employees' performance and facts within the scope of employment, the company's and employees' compliance with applicable laws and internal policies, and to ensure that reporting will not be considered a violation of employees' rights to honour, dignity and business reputation. It is also necessary to ensure that the rights of individuals to the protection (confidentiality) of their private life information remain unaffected by the whistleblowing procedures.

Confidential information and commercials secrets of third parties (clients, suppliers, etc.) should not be transferred as part of the whistleblowing program unless such third parties have given their consent for the transfer (the consent can either be included in a contract with the third party or obtained separately). The relevant restriction will also need to be inserted in the local whistleblowing policy.

State secrets (should any of the employees be admitted to state secrets within the scope of their work) should not be transferred.

44.8 Are there limits as to who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No.

44.9 Are there limits as to who can be a subject of a report?

Yes. The whistleblowing program can be implemented subject to the requirements outlined below.

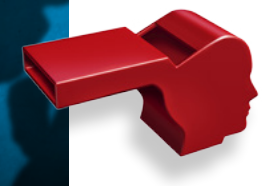
44.10 Is anonymous reporting permitted?

Yes. Anonymous reporting is allowed but not encouraged.

44.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes. General restrictions on the transfer of personal data apply.

An employee's prior written consent is essential for the transfer of personal data to third parties, including companies of the same group. The full names and addresses of such third parties shall be specified in the consent.



Considering that there will likely be a cross-border transfer of personal data during the whistleblowing program, all data subjects concerned should be requested to provide their prior consent for the transfer of their personal data to particular foreign legal entities and for the processing of the personal data by such entities. Technically, the form of consent for the cross-border transfer of data (written or oral) depends on the particular country where the data will be transferred and on the type of information to be transferred.

Still, from a practical perspective, the basic recommendation is to obtain written consents from employees for the processing of their personal data even if consent in an oral form is allowed by statute.

44.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

Yes. A prior written consent from each employee is required for the processing of their personal data in connection with the whistleblowing system (including consent for the data to be used by other employees for the purpose of whistleblowing); similarly, an employee's consent is required for the cross-border transfer of data and the transfer of third parties.

The consent for the personal data processing should include all necessary information specified in the Personal Data Law, including type of personal data to be processed, term of processing, forms and methods of processing, purposes of processing (all potential purposes should be included as the processing of personal data for a purpose not covered by the consent is illegal), any third parties to which personal data will be transferred, countries where the data may be transferred, etc.

Apart from obtaining written consents for the personal data processing, pursuant to the Labour Code, employees should acknowledge the local policy in writing after its adoption by the employer.

It should be, for completeness, noted that upon receipt of the reported information, the employer needs to commence an internal investigation in accordance with the Labour Code, which will include informing the employee(s) concerned of the report and a request for written explanations.

44.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

No. Should any trade union or other employees' representative body be formed within the company, the employer shall be obliged to consult with it before the adoption of certain local acts and policies as envisaged by Russian labour law. However, a whistleblowing policy is not listed among such acts and policies; thus, as a general rule, the employer (i.e., a Russian entity) does not need to consult with the trade union or other employees' representative body in order to adopt this policy.

However, the requirement for consultation may be specified in the collective bargaining agreement (if one was concluded). In particular, the collective bargaining agreement can require the employer to follow the procedure of consultation before the adoption of any local policy affecting the rights of the employees.

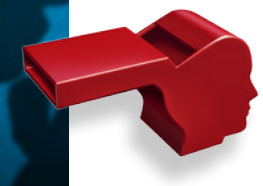
44.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

Yes. Companies introducing a whistleblowing program would need to undertake certain organizational and technical measures to protect personal data, including, among others, appointment of an employee responsible for the personal data protection and implementation of a personal data protection policy.

More importantly, the new data localization rules, which came into effect on September 1, 2015, (the Federal Law No. 242-FZ dated July 21, 2014, On Amendments to Certain Legislative Acts of the Russian Federation to Clarify the Procedure for Personal Data Processing in Information and Telecommunication Networks) can be relevant for the implementation of a whistleblowing program. According to these provisions, any database containing personal data of Russian nationals (including employees) that may be transferred abroad should be initially stored, maintained and updated at a server located in Russia.

For more information, contact:

Name: Anton Bankovskiy or Vladislav Eltovskiy
Firm: CMS Russia
Address: Presnenskaya nab. 10, 123317 Moscow, Russia
Telephone: +7 49 5786 4000
Fax: +7 49 5786 4001
Email: Anton.Bankovskiy@cmslegal.ru
Vladislav.Eltovskiy@cmslegal.ru
Website: www.cmslegal.ru



45. SERBIA

45.1 Applicable law and/or data protection guidelines?

The laws governing this area are the Law on Protection of Whistleblowers ("Official gazette of RS", No. 128/2014) and Personal Data Protection Law ("Official gazette of RS", Nos. 97/2008, 104/2009, 68/2012 and 107/2012).

An employer with 10 or more employees is required to have an internal whistleblower program in place, while other employers are only required to have a person authorized to receive whistleblower reports and conduct the internal proceedings.

In addition, the Serbian Criminal Code prescribes a general obligation for every person to notify the police if some actions have elements of a criminal offense, while the Law on Civil Servants prescribes an additional obligation for a civil servant to notify his/her superiors of any corruption-related information that has come to his/her attention.

45.2 Is an English translation available?

The Law on Protection of Whistleblowers is not available in English. An unofficial translation of the Personal Data Protection Law is available at:

www.poverenik.rs/images/stories/dokumentacija-nova/zakon-o-zastiti-podataka-o-licnosti_en.pdf

45.3 Is prior notification or approval required?

No.

45.4 Can notification or approval be filed online?

Not applicable.

45.5 Generally, how long does it take to get approval?

Not applicable.

45.6 Contact information for Data Protection Authority?

Name:	The Commissioner for Information of Public Importance and Personal Data Protection
Address:	Bulevar kralja Aleksandra 15, 11000 Belgrade, Serbia
Telephone:	+381 11 340 8900
Fax:	+381 11 334 3379
Email:	office@poverenik.rs
Website:	www.poverenik.rs

45.7 What is the scope of reporting permitted?

An individual can principally report on all violations of regulations or human rights, use of public authority contrary to its purpose, danger to human life, public health, security and the environment, and to prevent large-scale damages, provided that the report was made within one year from learning of the violation or, at the latest, within 10 years from the date the violation occurred, and provided that a person with an average knowledge and the experience of the whistleblower would believe in the truthfulness of the information, according to the data available at the time of reporting.

In addition, if any information being reported contains secret data, a whistleblower cannot disclose it to the public and is required to first notify his/her employer or employer's superior (if the information pertains to the employer), except in cases of direct danger to human life, public health, security or the environment, danger of large-scale damages or direct danger of destruction of evidence, when he/she is allowed to do so without prior notification.

45.8 Are there limits as to who can make a report under a whistleblowing program? (E.g. only managers and executives? Other employees? Suppliers?)

No, any individual can make a report.

45.9 Are there limits as to who can be a subject of a report?

No.

45.10 Is anonymous reporting permitted?

Yes, anonymous reporting is permitted.

45.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes, general restrictions on transfer of data as prescribed by the Personal Data Protection Law apply to whistleblowing programs as well (written consent of employees, consent of the Commissioner for Information of Public Importance and Personal Data Protection for transfer of data abroad).

45.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No, consent of employees is not required for a whistleblower program, but any creation of a special database for this purpose, including processing or transfer of personal data, must be in accordance with requirements prescribed by the Personal Data Protection Law.

45.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

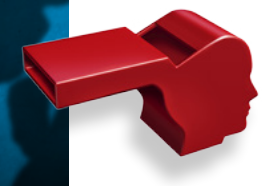
No.

45.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

No.

For more information, contact:

Name:	Radivoje Petrikić or Ksenija Ivetić Marlović
Firm:	Petrikić & Partneri AOD in cooperation with CMS Austria
Address:	Cincar Jankova 3, 11000 Belgrade, Serbia
Telephone:	+381 11 320 8900
Fax:	+381 11 303 8930
Email:	radivoje.petrikic@cms-rrh.com or ksenija.ivetic@cms-rrh.com
Website:	www.cms-rrh.com



46. SLOVAKIA[26]

46.1 Applicable law and/or data protection guidelines?

The Slovak Republic has no general whistleblower protection act. However, there is special legislation in the labour sector, where Act No. 307/2014 Coll. on Certain Measures Regarding Notifications of Antisocial Activities ("Act No. 307/2014") regulates the protection of employees against victimization in labour relations in relation to the notification of a crime or other antisocial activities. According to this Act, cooperation between the employer and the Labour Inspectorate is required in various situations. For example, an employer may take legal action or issue a decision against a protected employee (whistleblower) only with the prior consent of the Labour Inspectorate.

Furthermore, Slovak Data Protection legislation relies on the principles enshrined in Act No. 122/2013 Coll., on Protection of Personal Data ("Data Protection Act").

46.2 Is an English translation available?

No, there is no official translation available on the Data Protection Authority´s ("DPA") website.

46.3 Is prior notification or approval required?

In general, according to the Data Protection Act, the notification duty shall apply to all filing systems in which personal data are processed[27] by fully or partially automated means of processing. Special registration by the DPA is necessary only in case of automated filling systems processing special types of personal data such as biometric data or data necessary for protection of property or other interests of a controller (e.g., obtained by security cameras).

The notification duty does not apply to filing systems in which personal data are processed on the basis of the employment relationship.

Under Act No. 307/2014, designated employers (i.e., employers who employ at least 50 employees or an employer who is a public authority) are obliged to issue an internal regulation specifying the procedures for:

- The filing of a complaint;
- Examining complaints and authorizations of the person responsible for examining complaints;
- Maintaining the confidentiality of the identity of the person who filed the complaint;

[26] Slovakia is a member state of the European Union. If you are interested in the EU law requirements, please refer to the section on the European Union.

[27] For the purposes of the Data Protection Act, processing of personal data shall mean any operation or set of operations which is performed upon personal data – obtaining, collecting, distributing, recording etc.

- Keeping records of complaints and their examination[28] (three years from the date of receipt of the complaint);
- Notifying the person who filed the complaint with the result of its examination; and
- Processing of personal data given in the complaint (e.g., first name, surname and residence address of the whistleblower).

On the basis of the above, the employer that processes personal data pursuant to Act No. 307/2014 should not be subject to the notification duty to the DPA. However, it cannot be excluded that other employers using fully or partially automated filing systems, which are not governed by Act No. 307/2014, could still be subject to the notification duty to the DPA.

46.4 Can notification or approval be filed online?

Yes, the notification on automated filling systems can be filed to the DPA online. A template for the notification is published by the DPA on its website.

46.5 Generally, how long does it take to get approval?

In general, the controller is obliged only to provide notification of the existence of the filing system before the commencement of personal data processing.

46.6 Contact information for Data Protection Authority?

Name:	The Office for Personal Data Protection of the Slovak Republic
Address:	Hrani-ná 12, 820 07, Bratislava 27, Slovak Republic
Telephone:	+421 2 3231 3214
Fax:	+421 2 3231 3234
Email:	statny.dozor@pdp.gov.sk
Website:	http://dataprotection.gov.sk/uoou/en

46.7 What is the scope of reporting permitted?

The scope of reporting is any antisocial activity defined in the Act No. 307/2014 (e.g., specified crimes, administrative violations) of which the natural person has become aware in the exercise of his/her employment, profession, position or function, and which can significantly contribute or has contributed to the identification or investigation of serious antisocial activities or to identifying or convicting the offender.

[28] In the scope of: (i) date of receipt of complaint (ii) the name, surname and address of residence of the person who filed the complaint; in the case of an anonymous complaint, it shall be noted that it is an anonymous complaint (iii) the object of the complaint (iv) the outcome of complaint examination (v) a date of the end of complaint examination.

Reporting of antisocial activities is neither considered as a breach of a contractual obligation of discretion nor a violation of the confidentiality obligation, in the case of obligations arising from the exercise of employment, profession, position or function, nor is it a breach of an obligation of confidentiality regulated under special laws. However, provisions of Act No. 307/2014 do not affect the provisions of special laws on the protection of classified information, postal secrecy, commercial confidentiality, bank secrecy etc.

46.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No. Act No. 307/2014 regulates the conditions for providing protection to employees (including civil servants) against victimization in labour relations in connection with the reporting of crime or other antisocial activities.

46.9 Are there limits as to who can be a subject of a report?

No.

46.10 Is anonymous reporting permitted?

Yes. However, according to the Act No. 307/2014, the person who filed the complaint is typically notified with the result of the examination into the complaint, which of course would not be possible in case of anonymous reporting.

46.11 Are there restrictions on the transfer of data in a whistleblowing program?

There are no special restrictions on the transfer of data in a whistleblowing program; however, it is necessary to comply with general rules regarding transmission of data given in the Data Protection Act.

The transfer of data between the Slovak Republic and EU member states does not need to be approved by the DPA. Transfer of personal data to other third countries that do not ensure the adequate level of protection may be executed only if the controller adopts adequate safeguards for the privacy and fundamental rights and freedoms of individuals and the execution of corresponding rights. Such safeguards are given in the EU's Standard Contractual Clauses pursuant to a special regulation (Directive 95/46/EC).

46.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No. According to the Data Protection Act, the controller can process personal data without the data subject's consent if the purpose of the processing of personal data, group of affected persons and the list of personal data is stipulated in a special act, such as Act No. 307/2014.

According to the Data Protection Act, the controller shall also process personal data without the consent of the affected person, if:

- Processing of personal data is necessary for the fulfilment of an important task carried out in the public interest;
- Processing of personal data is necessary for the protection of rights and interests protected by law of the controller or the third party; this shall not apply if fundamental rights and freedoms of a data subject protected by this Act are predominant in such personal data processing; or
- Processed personal data have already been disclosed pursuant to the law and the controller properly marked them as disclosed.

46.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

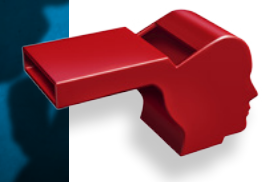
No. However on the basis of Act No. 307/2014, any actions of the employer against its employee (whistleblower) can be made only with the prior consent of the Labour Inspectorate. The Inspectorate will grant its consent only in the case that the employer proves that the proposed action has no causal connection with the notification (complaint) of the employee.

46.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

No.

For more information, contact:

Name: Michal Kohn
Firm: Ruži ka Csekes, in association with CMS Austria
Address: Vysoká 2/B, 811 06 Bratislava, Slovakia
Telephone: +421 2 3233 3444
Fax: +421 2 3233 3443
Email: michal.kohn@rc-cms.sk
Website: www.rc-cms.sk



47. SLOVENIA[29]

47.1 Applicable law and/or data protection guidelines?

In 2011, Slovenia passed the Integrity and Prevention of Corruption Act ("Zakon o integriteti in prepre-evanju korupcije", hereinafter "ZIntPK"), implementing the provisions on protection of whistleblowers in Slovenia. The ZIntPK provides solely for the protection of the whistleblower; it does not provide a notification or approval system for implementation of a whistleblowing program. Currently, there is no applicable law or guidelines under which a private or public entity would be either obliged to implement such a program or be subjected to obtaining an approval for implementation of a whistleblowing program. If a company wants to implement such a program, this could fall under the scope of the Employment Relationship Act ("Zakon o delovnih razmerjih") and the scope of protection of personal data under the Personal Data Protection Act (Zakon o varstvu osebnih podatkov, hereinafter the "DPL").

Under ZIntPK, the Commission for the Prevention of Corruption ("Komisija za prepre-evanje korupcije") was established. The ZIntPK provides that anyone can report an allegedly corrupt activity or other breach, which is then subject to investigation by the Commission. The identity of the whistleblower is protected and can only be disclosed by the court, if this would be necessary to ensure the public interest or rights of others. Further, ZIntPK also provides security for officials in the public sector. If they believe they are being requested or required to execute an illegal or unethical act and are, for this reason, subject to mental abuse or physical violence, they have the option to report the situation to their supervisor or an authorized person. The above-described whistleblowers are entitled to demand compensation in case of retaliatory measures and damages invoked.

47.2 Is an English translation available?

Yes. A translation of the ZIntPK is available at:
www.kpk-rs.si/upload/datoteke/ZintPK-ENG.pdf

Please note that the published translation does not include amendments of the ZIntPK published in the Official Gazelle of Republic of Slovenia on September 2, 2011 or later.

47.3 Is prior notification or approval required?

Please see the response to Question 47.1.

If the collection and processing of personal data will take place, a notification to the Information Commissioner is required at least 15 days before the data collection begins.

[29] Slovenia is a member state of the European Union. If you are interested in the EU law requirements, please refer to the section on the European Union.

47.4 Can notification or approval be filed online?

Not applicable.

Please note that the report of allegedly corrupt actions or other breaches under ZIntPK can be submitted through the form (available in Slovene only) provided at: www.kpk-rs.si/sl/nadzor-in-preiskave/prijava-suma-korupcije-in-drugih-nepravilnosti

47.5 Generally, how long does it take to get approval?

Not applicable.

47.6 Contact information for Data Protection Authority?

Under ZIntPK:

Name:	Komisija za prepre-evanje korupcije
Address:	Dunajska cesta 56, 1000 Ljubljana, Slovenia
Telephone:	+386 1 400 5710
Fax:	+386 1 478 8472
Email:	anti.korupcija@kpk-rs.si
Website:	www.kpk-rs.si

Under the DPL:

Name:	Information Commissioner (Informacijski pooblaš-enec)
Address:	Zaloška cesta 59, p.p. 78, SI-1000 Ljubljana, Slovenia
Telephone:	+386 1 230 9730 or +386 1 230 9778
Email:	gp.ip@ip-rs.si
Website:	www.ip-rs.si/?id=195

47.7 What is the scope of reporting permitted?

ZIntPK covers the following actions, which can be the subject of a report to the Commission: actions deemed as corrupt by the whistleblower, conflict of interest, accepting of gifts, declaration and supervision of assets of individuals. The scope of reporting permitted can cover all of the above or any individual action among those listed.

If the Commission concludes that the reported event contains elements of a criminal offense for which the offender is prosecuted ex officio, it will inform the law enforcement authorities with the request to keep the Commission informed. Further, the Criminal Code provides the obligation to report certain illegal acts; otherwise, the reporting individual could be found responsible for a criminal offense, such as failure to provide information of a crime or perpetrator.

47.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

Under ZIntPK, anyone is eligible to report an allegedly corrupt action or other violation to the Commission.

47.9 Are there limits as to who can be a subject of a report?

Under ZIntPK, the report on allegedly corrupt action or other breach can refer to either a legal entity in the private or public sectors, a state body, a body exercising public powers or an individual whose actions the whistleblower believes have the character of corruption.

47.10 Is anonymous reporting permitted?

The report can be submitted anonymously, but the Commission may be, in such case, unable to contact the whistleblower in order to obtain information necessary to successfully close the case.

47.11 Are there restrictions on the transfer of data in a whistleblowing program?

Under ZIntPK, the data (documents, evidence, etc.) is not considered public information until the end of the Commission investigation. The information on the whistleblower remains as non-public information after the conclusion of the investigation proceeding. ZIntPK does not provide further provisions in this regard.

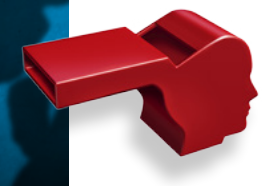
Should there be a whistleblowing program outside the scope of ZIntPK, and which would include personal data as defined by the DPL, the provisions of the DPL would need to be respected.

47.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

As explained in the response to Question 47.1 above, this is not explicitly regulated under Slovenian law. Thus, the implementation of an internal whistleblower program is not explicitly banned or, on the other hand, addressed in the legislation.

Usually such a program would be implemented in the framework of an employer's general acts. If this is the case, the employer would have to discuss the implementation of the program with any trade union involved. If there is no trade union, the proposed program should be given to the Works Council and/or the worker representative to obtain their opinion. If there is no trade union, Works Council and/or worker representative, the employees are solely to be notified of the implementation of such a program.

Should the data in question encompass personal data of employees, this would fall under the scope of the DPL and would require either adherence to the statute providing such transfer of data or the consent of each individual. Personal data is considered to be any data relating to an individual, irrespective of the form in which it is expressed.



47.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

Please see the response to Question 47.12.

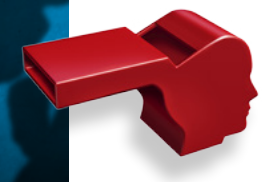
47.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

Under ZIntPK, no provisions on technical requirements are provided, whereas the processing of data collected is limited to the purpose of implementing the measures and methods as provided in the response to Question 46.9. The duration of storage of such data is limited to 10 years.

Under the DPL, the duration of storage of collected personal data is limited to as long as necessary to achieve the purpose for which the data were collected or further processed. The DPL further implies that after achieving the purpose of the data collection, the personal data should be erased, destroyed, blocked or anonymized unless the law provides otherwise. The DPL provides general safety requirements regarding the storage of the personal data. Organizational, technical and logical-technical procedures and measures to protect personal data, and to prevent accidental or deliberate unauthorized destruction, modification or loss of data, and unauthorized processing of such data should be ensured.

For more information, contact:

Name: Luka Fabiani
Firm: CMS Slovenia
Address: Bleiweisova 30, SI-1000 Ljubljana, Slovenia
Telephone: +386 1 6205 210
Fax: +386 1 6205 211
Email: luka.fabiani@cms-rrh.com
Website: www.cms-rrh.com



48. SOUTH AFRICA

48.1 Applicable law and/or data protection guidelines?

Yes. South Africa does have specific whistleblower protection laws in place designed to encourage and protect disclosures of wrongdoing in the public and private sectors.

The Protected Disclosures Act 26 of 2000 (the "PDA") protects employees as long as certain provisions are complied with in the disclosure. Essentially, a disclosure is protected if it contains information about impropriety and it has been made to the right person according to the scheme set out in the PDA.

Confidentially clauses in employment contracts and/or settlement/severance agreements are invalid insofar as they conflict with the PDA's protection.

Employees who make protected disclosures, are protected from adverse employment actions, referred to as "occupational detriment". This means:

- Being subject to discipline;
- Being dismissed, suspended, demoted, harassed or intimidated;
- Being transferred against his/her will;
- Being refused a transfer or promotion;
- Being subject to a term or condition of employment or retirement that is altered or kept altered to his/her disadvantage;
- Being refused a reference or being provided with an adverse reference from his/her employer;
- Being denied appointment to any employment or to any professional office;
- Being threatened with any of the actions as set out above; or
- Being otherwise adversely affected in respect of his/her employment or professional office including employment opportunities and work security.

It is important to note that the PDA only applies to employees, which excludes individuals such as contractors.

While the protection exists in practice, there have been numerous victimization examples in South Africa, and many view the protection offered by the PDA as simply "paper protection".

A further provision in South African law is Section 159 (7) of the South African Companies Act, 71 of 2008, which provides for a reporting mechanism. A public or state-owned company, must directly or indirectly establish and maintain a system to receive disclosures confidentially and act on them, and must routinely publicize the availability of that system to certain categories of persons as set out in this section. This section must be read with the PDA, as it is not a substitute for it. In terms of the section, a disclosure is protected if it is made in good faith, and to certain bodies such as legal advisors, directors, company secretaries, internal audit and the like.

This section goes much wider that the PDA in that shareholders, directors, company secretaries, prescribed officers as well as employees are protected in terms of this section. Furthermore, such individuals can claim damages from parties that cause them detriment, which includes threats of a detriment.

In South Africa, the right to privacy is protected in terms of the common law as well as Section 14 of the Constitution. The Constitutional right to privacy, like its common law counterpart, is not an absolute right, but may be limited in terms of laws of general application, and has to be balanced with other rights that are entrenched in the Constitution. The processing of personal information is also regulated in terms of Acts such as the Electronic Communications and Transactions Act, 25 of 2002, as well as the National Credit Act, 34 of 2005.

The Protection of Personal Information Act 4 of 2013 ("POPI") is South Africa's first attempt at specific data protection legislation. At the moment however, only certain sections are in force, such as the sections relating to the establishment of an information regulator and the making of regulations. The remaining sections will only commence once the President has determined the date for commencement. Furthermore, POPI also provides for a transitional period, so the processing of personal information will be required to comply with its provisions within one year of its commencement although it may be extended to three years on application. Accordingly, data protection in place in South Africa at the moment is weak, and the legislation does not directly address whistleblower or whistleblower information.

48.2 Is an English translation available?

The primary language is English.

48.3 Is prior notification or approval required?

No.

48.4 Can notification or approval be filed online?

Not applicable.

48.5 Generally, how long does it take to get approval?

Not applicable.

48.6 Contact information for Data Protection Authority?

Not yet available.

48.7 What is the scope of reporting permitted?

The Protected Disclosures Act 26 of 2000 (the PDA) protects employees as long as certain provisions are complied with in the disclosure. Essentially, a disclosure is protected if it contains information about impropriety and it has been made to the right person according to the scheme set out in the PDA. So, for example, a disclosure can be made to a legal practitioner for the purpose of obtaining advice about the employee's concerns and how to raise the concerns. A further requirement is that a disclosure to the employer must be made in good faith and follow the processes set out for such disclosures by the employer.

Disclosures made to the office of the Public Protector as well as to the office of the Auditor General are protected. In this instance, there is no requirement that the concern should firstly be raised with the employer. Finally, a generally protected disclosure is protected if it is made to the South African Police Services, members of Parliament and even the media.

For the protection to apply in this instance, the whistleblower must honestly and reasonably believe that the information and allegations contained in it are substantially true, and that the disclosure is not made for personal gain. Furthermore, there must be a good cause for going outside the normal channels and the particular disclosure must be reasonable. An example of good cause for going outside the normal channels would be if the concern was raised internally, but was not properly addressed. If it was not raised internally, the whistleblower must reasonably believe that he/she would be victimized or that a cover-up was likely.

Section 159 (7) of the South African Companies Act, 71 of 2008, also provides for a reporting mechanism.

To be protected, the person making the disclosure must reasonably believe at the time of the disclosure that the information showed or intended to show that a company or director or prescribed officer of the company had contravened the Companies Act, or was failing to comply with any statutory obligation to which the company was subject, or had engaged in conduct that had endangered or is likely to endanger the health or safety of individuals, or has harmed or is likely to harm the environment, among other provisions.

48.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

Yes, only employees under the PDA and shareholders, directors, company secretaries, prescribed officers as well as employees, under the Companies Act as described above, may report.

48.9 Are there limits on who can be a subject of a report?

Under the PDA, the disclosure must relate to impropriety in the workplace, i.e., the employer, or another employee of the employer.

Under the Companies Act, the disclosure must relate to the company or a director or prescribed officer of the company.

48.10 Is anonymous reporting permitted?

Yes.

48.11 Are there restrictions on the transfer of data in a whistleblowing program?

No. There are no specific provisions relating to whistleblower information. The normal provisions of privacy as set out above will apply.

48.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No.

48.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

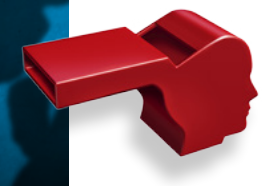
No.

48.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

No.

For more information, contact:

Name: Dave Loxton
Firm: ENSafrica
Address: 150 West Street, Sandton, Johannesburg, South Africa 2196
Telephone: +27 11 269-7600
Fax: +27 11 269 7899
Email: dloxton@ensafrica.com
Website: www.ensafrica.com



49. SOUTH KOREA

49.1 Applicable law and/or data protection guidelines?

While there is no general legislation in Korea governing whistleblowing programs, Korea has enacted the Act on the Protection of Public Interest Whistleblowers (the "Act") to protect whistleblowers who report on certain public interest issues. Issues of public interest include health, safety, environment, consumer protection and fair competition.

The collection, transfer and use of personal data in connection with a whistleblowing program will be subject to the Personal Information Protection Act ("PIPA"), which is the general law governing protection of personal information.

49.2 Is an English translation available?

No English translation of the Act is available. An unofficial English translation of PIPA can be found at http://elaw.klri.re.kr/eng_service/lawView.do?hseq=28981&lang=ENG

49.3 Is prior notification or approval required?

Notification to or approval from the regulatory authority is not required under the Act.

49.4 Can notification or approval be filed online?

Not applicable.

49.5 Generally, how long does it take to get approval?

Not applicable.

49.6 Contact information for Data Protection Authority?

The Anti-Corruption & Civil Rights Commission ("ACRC") has oversight and enforcement authority over the Act.

Name: ACRC (Anti-Corruption & Civil Rights Commission)
Address: Government Complex-Sejong, 20, Doum 5-ro, Sejong-si, Korea
Telephone: +82 44 200 7151~6
Website: www.acrc.go.kr

49.7 What is the scope of reporting permitted?

There is no defined scope of reporting.

49.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No.

49.9 Are there limits on who can be a subject of a report?

No.

49.10 Is anonymous reporting permitted?

Yes.

49.11 Are there restrictions on the transfer of data in a whistleblowing program?

No, but this will be subject to the requirements for transfer of personal information under PIPA if personal information is included in the data being transferred.

49.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No, employees' consent is not required for a whistleblowing program. However, to the extent the data in the whistleblowing program contains the employee's personal data, PIPA will apply and the requirements under PIPA must be complied with.

49.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

No.

49.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

No. However, if the reported information contains personal data, PIPA will apply and adequate security controls must be in place to disable any recovery or recycling of the personal data.

For more information, contact:

Name: Taeuk Kang
Firm: Bae, Kim and Lee LLC
Address: Hyundai Marine & Fire Insurance Bldg. 17F, 137 Teheranro, Gangnamgu, Seoul
Telephone: +82 2 3404 0485
Fax: +82 2 3404 0001
Email: taeuk.kang@bkl.co.kr
Website: www.bkl.co.kr

50. SPAIN[30]

50.1 Applicable law and/or data protection guidelines?

No, Spain has no specific whistleblower protection laws in place.

Whistleblower programs have been regulated by the Data Protection Authority's ("DPA) guidelines, in particular by the "Guide for Data Protection in Labour Relationships"; visit www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php and scroll down to find "Guía 'La protección de datos en las relaciones laborales' – 2009: Versión en inglés"

and the DPA report no. 128/2007; see: www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2007-0128_Creaci-oo-n-de-sistemas-de-denuncias-internas-en-las-empresas-mecanismos-de-whistleblowing.pdf.

50.2 Is an English translation available?

No.

50.3 Is prior notification or approval required?

No. However, there is always a general obligation to (i) notify the DPA about the existence of a data file containing the personal data derived from the whistleblowing program and (ii) if there is a transfer of personal data outside the EU/EEA, the obligation to apply for and obtain an express authorization from the DPA.

50.4 Can notification or approval be filed online?

Not applicable.

50.5 Generally, how long does it take to get approval?

Not applicable.

50.6 Contact information for Data Protection Authority?

Name:	Spanish Data Protection Authority (Agencia Española de Protección de Datos)
Address:	C/ Jorge Juan, 6, 28001 Madrid, Spain
Telephone:	+34 901 10 0 099
Email:	See website
Website:	www.agpd.es

[30] Spain is a member state of the European Union. If you are interested in the EU law requirements, please refer to the section on the European Union.

50.7 What is the scope of reporting permitted?

In principle, no specific material restrictions are contemplated. Nonetheless, as a general principle, any such program must be proportionate and connected with the interests of the company, without unnecessarily invading the privacy of the affected individuals.

50.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No. As a general principle, companies are free to design their programs as they deem appropriate, without applying any specific regulatory restriction in this respect.

50.9 Are there limits on who can be a subject of a report?

No. As a general principle, companies are free to design their programs as they deem appropriate, without applying any specific regulatory restriction in this respect.

50.10 Is anonymous reporting permitted?

No. Pursuant to the criteria set forth by the DPA's guidelines, the reporter must always be identified by the manager of the program. This is aimed at avoiding indiscriminate or arbitrary complaints.

50.11 Are there restrictions on the transfer of data in a whistleblowing program?

No. The only restrictions are those deriving from the general provisions set forth in the law. Any international transfer or communication of personal data must be done in full compliance with the provisions of the Spanish Data Protection Act and related regulations, as summarized below:

i. Communication of personal data to third parties: Spanish regulations set forth that the express and informed consent of the affected individual must be obtained before such communication is conducted.

ii. International transfers: If the entity to which the personal data is going to be communicated is 1) established in the EU or 2) is established in a country granting a similar protection to personal data as the one provided by the Spanish regulations, the international transfer can be made to the extent that:

   a) The affected individuals are informed in advance about the identity of the third party gaining access to their personal data and, when applicable, they consent to such access; and

   b) A notification of the international transfer is filed with the DPA.

If the owner of the personal data is not included in one of the categories mentioned in ii above, the international transfer may be done as long as the following requirements are met:

a) The affected individuals are informed in advance about the identity of the third party gaining access to their personal data and, when applicable, they consent to such access; and

b) Express and prior authorization is given by the director of the DPA.

50.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No. However, the employees must be informed in advance and in detail about the implementation of a whistleblower program. Regarding the transfer of their personal data, please see comments to question 50.11 above.

50.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

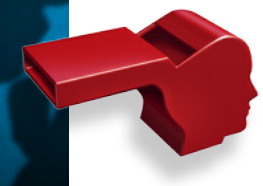
The company has to inform a Works Council on any issue that may have an impact on its employees. Hence, the launching of this kind of program falls within the scope of this obligation, requiring the company to inform said council on the main features of the program to be launched.

50.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

No. Apart from the general obligations set forth by Spanish data protection laws, including the implementation of the mandatory high-level security measures required by the Spanish laws, there are no specific regulations dealing with the whistleblower program. In particular, with respect to deletion, according to Spanish law, the personal data must be cancelled when no longer necessary or appropriate for the purpose for which they were collected or registered).

For more information, contact:

Name: Jorge Llevat or Jorge Monclús
Firm: Cuatrecasas, Gonçalves Pereira
Address: Paseo de Gracia 111, 08008 Barcelona, Spain
Telephone: +34 93 2905 585
Fax: +34 93 2905 569
Email: jorge.llevat@cuatrecasas.com or jorge.monclus@cuatrecasas.com
Website: www.cuatrecasas.com



51. SWEDEN[31]

51.1 Applicable law and/or data protection guidelines?

No, Sweden has no specific whistleblower protection laws in place.

Whistleblowing reports may include data regarding violations of law and/or criminal allegations. According to Section 21 of the Swedish Personal Data Act, such data about violations or criminal allegations may only be processed by the Swedish authorities. Therefore, the implementation of some whistleblowing programs may violate Swedish law.

According to a statute issued by the Data Protection Authority ("DPA") and effective November 1, 2010, there is no longer a requirement to apply to the DPA for an exemption for notification of a whistleblowing scheme. However, the requirements for how companies manage and process personal data in the system are the same as before, i.e.:

- The whistleblowing scheme must be a supplement to the company's normal internal management and administration and its use must be voluntary. The system may only be used when non-use of the company's internal information and reporting channels is justifiable on objective grounds.
- The whistleblowing scheme must be limited to serious irregularities concerning accounting, internal accounting control, auditing matters, the fight against bribery and banking and financial crimes. The system may also be used for other serious irregularities concerning the company's vital interests or the life and health of individuals.
- Only key personnel and employees in a management position may be reported on and only they may be processed in the system.
- The company is obliged to ensure that the processing for which the company is responsible is in compliance with the Swedish Personal Data Act, for example in relation to the processing of sensitive personal data, information to the employees and transmission of personal data to third countries.

51.2 Is an English translation available?

No.

51.3 Is prior notification or approval required?

No, there is no need for an approval or exemption provided that the requirements are fulfilled as set out in the answer to Question 51.1 above.

[31] Sweden is a member state of the European Union. If you are interested in the EU law requirements, please refer to the section on the European Union.

An exemption would be required if the company wishes to deviate from the requirements set out in the answer to Question 51.1 (e.g., to process data in relation to other than key employees or employees in a management position. However, neither the Swedish DPA nor the Swedish courts have approved any deviations from the requirements set out in Question 51.1 above.

As a general rule, the processing must be notified to the DPA unless the company has appointed a Data Protection Officer, in which case it is possible to claim the right to use an exception in order to avoid notification. We, however, recommend a notification be filed.

51.4 Can notification or approval be filed online?

No.

51.5 Generally, how long does it take to get approval?

No approval is required if the requirements are fulfilled set out in the answer to Question 51.1 above. However, if an application for exemption is needed (i.e., when the whistleblowing program does not fulfil the requirements set out above), it would usually take less than three months.

51.6 Contact information for Data Protection Authority?

Name:	Datainspektionen
Address:	Drottninggatan 29, plan 5, Box 8114, 104 20 Stockholm, Sweden
Telephone:	+46 08 657 61 00
Email:	datainspektionen@datainspektionen.se
Website:	www.datainspektionen.se

51.7 What is the scope of reporting permitted?

The whistleblowing-scheme must be limited to serious irregularities concerning accounting, internal accounting control, auditing matters, the fight against bribery and banking and financial crimes. The system may also be used for other serious irregularities concerning the company's vital interests or the life and health of individuals.

51.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No. However, use of the whistleblowing program must be voluntary.

51.9 Are there limits on who can be a subject of a report?

Yes. Only key personnel and employees in a management position may be subjects of a report and only such employees may be processed in the system.

51.10 Is anonymous reporting permitted?

Yes.

51.11 Are there restrictions on the transfer of data in a whistleblowing program?

No, there are no specific restrictions on the transfer of data in the whistleblowing program. The regulation concerning whistleblowing pertains only to the processing of data including criminal allegations etc. within the whistleblowing program.

The transfer of data to third countries is subject to the same provisions as if the data was not processed within the scope of the whistleblowing program. However, the use of Binding Corporate Rules requires the DPA's approval.

51.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No. However, exemptions from the requirement of consent may apply subject to considerations in the specific matter. If consent can be obtained, it is normally recommended. A transfer to third countries must be based on consent, EU Standard Contractual Clauses or any other adequate security level.

51.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

Yes. In general, there is likely an obligation to negotiate with a Works Council, union or other employee representative group; however, it depends on the structure of the whistleblowing system.

There is also an obligation to notify the union (if applicable). Such notification must be made prior to implementing the whistleblowing program.

51.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

No. A general requirement is that personal data may not be stored longer than necessary with regard to the purpose of the processing.

For more information, contact:

Name:	Fredrik Roos or Bobi Mitrovic
Firm:	Setterwalls Advokatbyrå AB
Address:	Sankt Eriksgatan 5, P.O. Box 11235, SE-404 25, Gothenburg, Sweden
Telephone:	+46 31 701 1700
Fax:	+46 31 701 1701
Email:	fredrik.roos@setterwalls.se or bobi.mitrovic@setterwalls.se
Website:	www.setterwalls.se

52. SWITZERLAND

52.1 Applicable law and/or data protection guidelines?

Switzerland has no specific whistleblower protection laws in place.

Various guidelines exist, but all of them on a private level.

52.2 Is an English translation available?

Not applicable.

52.3 Is prior notification or approval required?

Not applicable.

52.4 Can notification or approval be filed online?

Not applicable.

52.5 Generally, how long does it take to get approval?

Not applicable.

52.6 Contact information for Data Protection Authority?

Name:	Eidgenoessischer Datenschutz und Oeffentlichkeitsbeauftragter
Address:	Feldeggweg 1, 3003 Bern, Switzerland
Telephone:	+41 31 322 43 95
Website:	www.edoeb.admin.ch

52.7 What is the scope of reporting permitted?

An overview of various private whistleblowing programs reveals that employees are encouraged to report any misconduct, deplorable circumstances, deficiencies, etc.

52.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No. As whistleblowing is a privately implemented concept in Switzerland, it depends on the employers whose whistleblowing reports they are going to accept.

52.9 Are there limits on who can be a subject of a report?

No.

52.10 Is anonymous reporting permitted?

Yes.

52.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes. Switzerland's Data Protection Law is equivalent to the protection awarded through the European Directive.

52.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No, employee consent is not necessary to implement a whistleblower program.

The transfer of data is subject to data protection legislation. Transfer to EU countries is permitted without consent, because the EU and Switzerland regard each other's data protection level as equivalent.

If neither of the above apply, consent may be required, depending on whether the reported conduct is a criminal offense (where there is a possibility of no consent being required but note the details are tricky), or only a misconduct regarding private company guidelines (consent necessary).

52.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

Not applicable.

52.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

The provisions of the data protection legislation apply, which require a high security level for personal data, in particular for sensitive data. Much employee data qualifies as sensitive (sex, religious beliefs, health data, etc.).

For more information, contact:

Name. Dr. Robert G. Briner,
Firm: CMS Switzerland
Address: Dreikönigstrasse 7, 8002 Zurich, Switzerland
Telephone: +41 44 285 1111
Fax: +41 44 285 1122
Email: robert.briner@cms-veh.com
Website: www.cms-veh.com

53. TAIWAN

53.1 Applicable law and/or data protection guidelines?

There is no specific statute governing whistleblowing in Taiwan. Relevant provisions are scattered over various Acts, mostly related to employment; for example, Act for Gender Equality of Employment, Labour Standards Act, Labour Safety and Health Act, Labour Inspection Act, Labour Pension Act.

Other than the above employment-related Acts, the Taiwan Stock Exchange and the Taipei Exchange promulgated Ethical Corporate Management Best Practice Principles and Guidelines for the Adoption of Codes of Ethical Conduct for listed companies, which request the establishment of whistleblowing program for violation of laws, regulations, codes of business conduct or integrity.

On the other hand, there is a Personal Information Protection Act, which deals exclusively with data protection. Data protection is considered a separate regime from whistleblowing though there may be some overlap.

53.2 Is an English translation available?

An English translation of the Personal Information Protection Act is available at: http://law.moj.gov.tw/Eng/LawClass/LawContent.aspx?PCODE=I0050021

53.3 Is prior notification or approval required?

No.

53.4 Can notification or approval be filed online?

Not applicable.

53.5 Generally, how long does it take to get approval?

Not applicable.

53.6 Contact information for Data Protection Authority?

There is no single data protection authority. Various central Ministries and city/county governments serve as the competent authorities of data protection within their own jurisdictions.

53.7 What is the scope of reporting permitted?

Whistleblowing programs are generally adopted by companies for the reporting of violations of laws, regulations, codes of business conducts or integrity.

53.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No.

53.9 Are there limits on who can be a subject of a report?

No.

53.10 Is anonymous reporting permitted?

For a report of sexual harassment, the person making the report must be named, as is required by the secondary legislation of the Act for Gender Equality of Employment. As to other types of reports, there is no specific legal requirement, and therefore such a report can be anonymous. But, in practice, named reporting is encouraged or requested (for example, as set forth in the Sample Template for the Procedure for Ethical Management and Guidelines for Conduct as published by the Taiwan Stock Exchange and the Taipei Exchange).

53.11 Are there restrictions on the transfer of data in a whistleblowing program?

It is subject to the notice given in the whistleblowing program. Further, if the personal data is to be transferred internationally, the competent authority of data protection may restrict such transfer:

- If it involves major national interests;
- Where an international treaty or agreement specifies otherwise;
- Where the country receiving personal data lacks proper regulations that protect personal data, which might harm the rights or interests of the data subject; or
- Where the international transfer of personal data is made through an indirect method in order to evade the provisions of the Personal Information Protection Act.

53.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No, but the employee must be notified of the transfer of data when the employer gives the prior notice of collection to the employee as required by the Personal Information Protection Act.

53.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

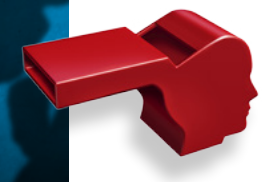
No.

53.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

No.

For more information, contact:

Name:	Chun-yih Cheng
Firm:	Formosa Transnational Attorneys at Law
Address:	13th Floor, Lotus Building, 136 Jen Ai Road Section 3, Taipei 10657, Taiwan
Telephone:	+886 2 2755 7366
Fax:	+886 2 2708 6035
Email:	chun-yih.cheng@taiwanlaw.com
Website:	www.taiwanlaw.com



54. THAILAND

54.1 Applicable law and/or data protection guidelines?

There is no specific whistleblower protection law in place in Thailand. Section 108 of the Labour Protection Act requires that a company has in place a system for lodging grievances, but does not provide any details as to what that system must include. Similarly, there is no single Data Protection Authority. Generally, Data Protection is covered under the following Laws:

- Civil and Commercial Code ("CCC");
- Computer Crimes Act B.E. 2550 (2007);
- Official Information Act B.E. 2540 (1997); and
- Labour Protection Act B.E. 2541 (1998) as amended.

Thailand has been a full participant of the Organization for Economic Co-operation and Development (OECD) Development since 2005. The country observes the OECD's Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data.

Thailand is in the process of drafting a Data Protection Bill. There is not a reference to a whistleblower protection program in the Bill, as currently under review by the Cabinet.

54.2 Is an English translation available?

Not applicable.

54.3 Is prior notification or approval required?

Not applicable.

54.4 Can notification or approval be filed online?

Not applicable.

54.5 Generally, how long does it take to get approval?

Not applicable.

54.6 Contact information for Data Protection Authority?

Not applicable.

54.7 What is the scope of reporting permitted?

Whistleblowing programs may be incorporated in business practices by any company operating in Thailand with any scope, as desired by that company. Note that this is not a legal requirement, and there are no specific laws that dictate any requirements or prohibitions.

54.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

See the response to Question 54.7.

54.9 Are there limits to who can be subject of a report?

See the response to Question 54.7.

54.10 Is anonymous reporting permitted?

See the response to Question 54.7.

54.11 Are there restrictions to the transfer of data in a whistleblowing program?

See the response to Question 54.7.

54.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

See the response to Question 54.7.

54.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

Not applicable.

54.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

There are no specific requirements other than retention of computer traffic records for at least 90 days by a computer network system administrator to meet statutory requirements for official requests for backtracking investigations under the Computer Crimes Act, 2007.

For more information, contact:

Name: Niwes Phancharoenworakul or Christopher Kalis
Firm: Chandler & Thong-ek Law Offices
Address: 7th-9th Fl., Bubhajit Building, 20 North Sathorn Rd, Bangkok 10500, Thailand
Telephone: +662 266-6485 thru 6510
Fax: +662 266-6483, 266-6484
Email: niwes@ctlo.com, or chris@ctlo.com

55. TURKEY

55.1 Applicable law and/or data protection guidelines?

No. Turkey has no specific whistleblower protection laws in place.

As for the applicable legal framework to data protection-related matters, Turkey ratified the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention No. 108") on February 18, 2016, which ultimately led to passage of the Data Protection Law (the "DPL") on March 24, 2016. The DPL entered into force on April 7, 2016 upon its publication in the Official Gazette, except for certain provisions of the DPL that shall become effective at a later date as designated by the law itself.

The DPL has been prepared to meet Turkey's obligations under the Convention No. 108 and is largely based on European Union Directive 95/46/EC. The DPL provides key definitions such as personal data, processing of personal data, data controller, data processor, explicit consent, and anonymization, and it also sets forth the principles for the processing of personal data, as well as the obligations of the data controller.

In addition to the DPLL, general principles of the Constitution of the Republic of Turkey, the Turkish Civil Code, the Turkish Code of Obligations, the Turkish Commercial Code, the Turkish Criminal Code and other applicable secondary legislations are also applicable to data protection-related matters.

Turkey also became a party to the United Nations Convention against Corruption in 2006 and promised to endeavor to establish and promote effective practices aimed at the prevention of corruption. However, no whistleblowing or similar mechanisms have been adopted to date.

55.2 Is an English translation available?

There is no publicly available English translation of the DPL.

55.3 Is prior notification or approval required?

In cases where information to be transferred to abroad within the scope of the implementation of a whistleblowing program is regarded as "personal data" or "sensitive personal data", explicit consent of the data subject must be obtained. If it is not possible to obtain such explicit consent of the data subject, one of the exceptions set forth under the DPL must be existent and (a) the respective foreign country must ensure an adequate level of protection or (b) written commitments of the controllers in Turkey and in the relevant foreign country regarding adequate protection and the Data Protection Authority's ("DPA") approval must be in place.

Moreover, in situations where the interests of the Republic of Turkey or the data subject may seriously be harmed, personal data may be transferred abroad only after obtaining an opinion from the relevant public authority and permission from the DPA, without prejudice to any international conventions.

55.4 Can notification or approval be filed online?

The DPL does not provide for an online notification or approval mechanism. However, such mechanism may be provided by the secondary legislation, which is expected to come into force within a year of the enactment of the DPL.

55.5 Generally, how long does it take to get approval?

Since the DPA will be formed within six months following the enactment the DPL, it is not possible at this time to predict timing for obtaining the approval of the DPA.

55.6 Contact information for Data Protection Authority?

This is not currently available as the DPA is yet to be established.

55.7 What is the scope of reporting permitted?

There is no limitation on the scope of reporting. However, if the reporting includes sensitive data, namely, data relating to persons' ethnic groups, political views, philosophical or religious views, racial origins, sexual orientation or life, health conditions or memberships with trade unions, it is obligatory to obtain the full consent of the concerned person. Otherwise, the storage of such sensitive information constitutes a crime. Also, even if the reporting is made upon obtaining the consent of the respective person, it may constitute a crime under certain circumstances, particularly, if the individual providing consent waived a fundamental personal right by giving such consent. In this regard, the *Turkish Criminal Code* imposes sanctions (which include imprisonment) in case of violation of private life, unlawful recording of personal data, unlawful collection of personal data, and unlawful storage of personal data.

Moreover, under the DPL, processing of sensitive personal data requires controllers to take adequate precautions together with obtaining the relevant person's consent. Since the DPA is yet to be established, the scope of these "adequate precautions" remains unclear for the time being.

55.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No.

55.9 Are there limits to who can be subject of a report?

No.

55.10 Is anonymous reporting permitted?

Yes, provided that the anonymous reporter should not have gained the reported information through unlawful means and the reported information reflects the truth.

55.11 Are there restrictions to the transfer of data in a whistleblowing program?

Yes.

Firstly, transfer of data is protected at the constitutional level. Article 20 of the Constitution of the Republic of Turkey requires full consent of the concerned person for transfer of personal data: *"Every individual has the right to request the protection of his or her personal data. This right encompasses being informed about the personal data, being able to reach to the data, and being able to request the data to be corrected or deleted. Personal data shall only be processed under the circumstances designated by the law or through the **explicit** consent of the concerned person."*

In line with the Constitution, the DPL also requires explicit consent of the relevant individual for transfer of his/her personal data. However, certain exceptions are listed under the draft law in an exhaustive manner and no consent must be sought in such cases for transfer of personal data.

Secondly, Article 75 of the Labour Law requires employers to follow good faith principle in disclosing information of their employees. Accordingly, employers are obliged to use the information that they possess regarding their employees in compliance with the principles of good faith and in accordance with the law and not to disclose any information in case the employee has interest for such information to remain confidential.

Additionally, Article 419 of the Turkish Code of Obligations allows the employer to use employees' data only to the extent it is required for performance of the employment agreement or disposition of the employee towards his/her work.

55.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

Obtaining an employee's written consent about the overall system and the transmission/storage of the employee's personal data is recommended before implementing the program.

55.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

Yes, but only if there is a collective bargaining agreement in place that requires that the trade union be consulted in the matter.

55.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

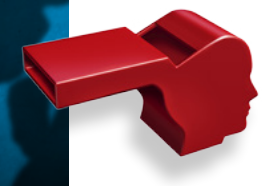
The DPL imposes an obligation on the data controller to take all kinds of technical and administrative safety precautions to prevent illegal processing, unlawful access, and preservation of personal data. In the event that personal data is processed by other individuals or corporations on behalf of the data controller, then the data controller will be jointly liable for taking these precautions. The DPL also requires data controllers to undertake audits to ensure compliance with these precautions.

As for the deletion of the reported information, the DPL stipulates that in the event the reasons for which the personal data were being processed are no longer valid, despite being processed in line with the applicable legislation, personal data will be erased, destroyed or anonymized by the controller *ex officio* or upon the demand of the data subject.

In light of the above, it would be critical to establish a policy for securely keeping and deleting reported information as leakage of such information may harm the reporting party or any relevant parties including the company.

For more information, contact:

Name: Kemal Mamak or Kayra Üçer
Firm: Hergüner Bilgen Özeke Attorney Partnership
Address: Büyükdere Caddesi 199, Levent 34394, Istanbul, Turkey
Telephone: +90 212 310 1800
Fax: +90 212 310 1899
Email: kmamak@herguner.av.tr or kucer@herguner.av.tr
Website: www.herguner.av.tr



56. UKRAINE

56.1 Applicable law and/or data protection guidelines?

Ukraine has no separate whistleblower protection law in place.

However, a number of laws contain provisions on protection of whistleblowers.

The Law of Ukraine "On Access to Public Information" provides that state service officials and officials of legal entities engaged in public information management shall, despite the breach of their non-disclosure duties, be exempt from liability for reporting information on violations of law or information about threat to people's health or safety or to the environment, if such officials act in good faith and reasonably believe that the information is trustworthy and contains evidence of a reported violation or reveals substantial damage to people's health, safety or environment.

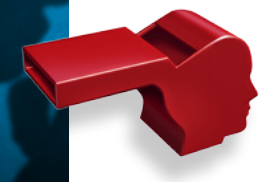
The Law of Ukraine "On Prevention of Corruption" (the "Anti-Corruption Law") includes guarantees to whistleblowers reporting on corrupt practices. In particular, whistleblowers and members of their families shall not be fired, threatened to be fired or forced to resign, neither shall any disciplinary action or other adverse measure (e.g., transfer to another place of work, change of working conditions, salary cut, etc.) be undertaken in relation to whistleblowers by their supervisors or employers as a result of such reporting by a whistleblower. Furthermore, where a whistleblower's life, health, dwelling or other property is in danger, a whistleblower may be protected by law enforcement authorities. Such protection shall be rendered to whistleblowers in the same manner as to individuals protected in the course of criminal proceedings (i.e., providing of security services, change of personal documents, relocation etc.).

According to the Anti-Corruption Law, any company may adopt an anti-corruption program and include provisions on whistleblowing therein. However, adoption and implementation of the anti-corruption program is obligatory for the following categories of companies:

1. A state-owned or municipal company or business (where the state or local authorities hold more than a 50% share) with an average number of more than 50 employees (per previous financial year) and over UAH 70 million (or approximately USD 2,700,000 as of February 2016) of gross sales for such period; and

2. A company engaged in public procurement if the cost of procurement is equal to or exceeds UAH 20 million (approximately USD 770,000).

In any event, the whistleblowing procedures shall not breach the Law of Ukraine "On Protection of Personal Data" (the "Data Protection Law"). The Data Protection Law defines personal data and establishes the rules for storing and processing of such data.



56.2 Is an English translation available?

No English translation is available.

56.3 Is prior notification or approval required?

No, no notification to, or approval of, any regulatory authority is required for setting up a whistleblower program.

If the whistleblower program includes processing of sensitive personal information (i.e., racial, ethnic and national origin; political, religious or world outlook; membership in political parties and/or organizations, trade unions, religious organizations and NGOs; health condition; sexual life; biometric data; genetic data; prosecution for committing administrative or criminal offenses; measures taken regarding the person in the course of prejudicial inquiry and investigation; violence committed against the person; location and movement of the person), such processing shall be notified to the Ukrainian Parliament Commissioner for Human Rights (the Ombudsman) within 30 working days after the commencement of processing.

56.4 Can notification or approval be filed online?

No. However, notification on processing of sensitive personal information (as explained above) may be sent to the relevant authority via e-mail.

56.5 Generally, how long does it take to get approval?

Not applicable.

56.6 Contact information for Data Protection Authority?

Name:	Ukrainian Parliament Commissioner for Human Rights
Address:	21/8 Instytutska St., 01008, Kyiv City, Ukraine
Telephone:	+380 44 253 1135; +380 44 253 53 94; +380 44 253 8194
Email:	hotline@ombudsman.gov.ua
Website:	www.ombudsman.gov.ua

56.7 What is the scope of reporting permitted?

There is no specific regulation in that respect. However, the processing and/or use of information obtained within a whistleblower program shall not be in conflict with the Data Protection Law.

56.8 Are there limits as to who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No.

56.9 Are there limits as to who can be a subject of a report?

No.

56.10 Is anonymous reporting permitted?

Yes. According to the Anti-Corruption Law, notification on corrupt practices may be made anonymously. In order for notification to be accepted for consideration by a responsible person or authority, such anonymous notification should contain information regarding the particular offender and facts that may be verified.

56.11 Are there restrictions on the transfer of data in a whistleblowing program?

According to the Data Protection Law, the controller of personal data can transfer the personal data for processing to managers of personal data, i.e., other natural persons or legal entities, including those residing abroad. Transfer of personal data abroad is possible when (i) there is an agreement between the controller and the manager and (ii) either the manager resides in the country that guarantees a proper level of personal data protection or the person whose data is processed consents to its transfer abroad.

State parties to the Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data of 1981 are considered to be the states with a proper level of personal data protection. If a state is not a party to this Convention, but a person whose personal data is processed consents to its transfer to any foreign managers, such transfer shall be construed legal as well.

The personal data may be transferred without consent of the person whose data is processed only in cases envisaged by law where it serves protection of national security, welfare and human rights.

56.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

The whistleblower program may be a part of a more complex anti-corruption program adopted in the company. The anti-corruption program should be discussed with employees before its adoption.

56.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

See our answer to question 56.12 above.

56.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

According to the Data Protection Law, personal data controllers and managers shall ensure that personal information is safely stored and shall prevent unauthorized access to it as well as prevent accidental or intentional loss or destruction thereof. Relevant organizational and technical security measures should be undertaken. In particular, personal data controllers and managers shall keep records regarding processing of personal data; establish procedures for the access of personal data by their employees; procedures for keeping records regarding the processing of personal data; elaborate an action plan for cases of unauthorized access, damage to technical facilities, and other emergency situations; provide training for the employees in charge; maintain the list of such employees; determine the access level for them, etc. In case of destruction of personal data at the request of an individual or where required by law, the personal data should be destroyed in a manner preventing its possible restoration in future.

For more information, contact:

Name: Maria Orlyk or Kateryna Soroka
Firm: CMS Ukraine
Address: 19-B Instytutska, 5th Floor, 01021 Kyiv, Ukraine
Telephone: +380 44 500 1710 or +380 44 500 1711
Fax: 380 44 500 1716
Email: maria.orlyk@cms-rrh.com or kateryna.soroka@cms-rrh.com
Website: www.cms-rrh.com

57. UNITED KINGDOM[32]

57.1 Applicable law and/or data protection guidelines?

Yes, the U.K. has specific whistleblower protection laws in place.

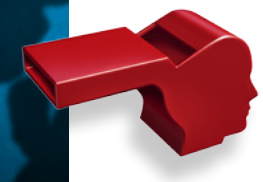
The Public Interest Disclosure Act 1998 ("PIDA"), which amends the Employment Rights Act 1996, came into force on July 2, 1999, and provides protection for workers who report malpractices by their employers or third parties against detriment and/or dismissal. Since the PIDA came into force, there have been further changes introduced under the Enterprise and Regulatory Reform Act 2013 ("ERRA").

To be a protected disclosure, the disclosure must be a "qualifying disclosure" of "information" made in accordance with one of the specified methods. Broadly, this is where there has been a disclosure of information that a worker reasonably believes is made in the public interest and tends to show malpractice is, has or is about to take place within an organization. PIDA encourages disclosures to be made internally to the employer rather than externally to a third party. More stringent conditions must be met for an external disclosure to be protected.

Note that the whistleblowing legislation in the U.K. imposes no positive obligations on employers to encourage whistleblowing or to implement a whistleblowing policy, save for listed companies where there is a positive obligation to maintain a sound system of internal control under the U.K. Corporate Governance Code, and public bodies where the government expects these to be in place. It merely requires them to refrain from subjecting whistleblowers to any detriment, including dismissal, provided their activities fall within the scope of a "protected disclosure". Having said that, employers can be vicariously liable where their employees victimize a whistleblowing colleague so it is good practice (although not a legal requirement) to have a policy in place.

If an employee is dismissed for the principal reason that they made a protected disclosure, that dismissal will be automatically unfair. There is also no cap on compensation in whistleblowing claims, unlike basic unfair dismissal claims. However, recent changes in legislation allow the compensation awarded to be reduced by up to 25% if the protected disclosure is not made in "good faith".

U.K. Employment Tribunals have the power to send details of an individual's whistleblowing claim to a prescribed person if the claimant gives his/her express consent (simply by ticking a box on the claim form). There are a large number of prescribed persons, which includes the U.K. Information Commissioner (our data protection watchdog). The U.K. government department for Business Innovation & Skills has recently published a comprehensive list of these "prescribed persons" which is available online. These prescribed persons will then



[32] The United Kingdom is a member state of the European Union. If you are interested in the EU law requirements, please refer to the section on the European Union.

have the opportunity to decide whether the issue highlighted in the claim form requires investigation. This will not, however, impact on the Employment Tribunal claim.

The government has indicated that it will be introducing new protections for public sector whistleblowers including applicants who wish to apply for positions in the National Health Service who have or are thought to have previously been whistleblowers. The government is also looking at putting in place further protections for whistleblowers in the financial services sector.

57.2 Is an English translation available?

The primary language is English.

The Employment Rights Act 1996:
www.legislation.gov.uk/ukpga/1996/18/contents

57.3 Is prior notification or approval required?

No.

57.4 Can notification or approval be filed online?

Not applicable.

57.5 Generally, how long does it take to get approval?

Not applicable.

57.6 Contact information for Data Protection Authority?

Name:	Information Commissioner's Office
Address:	Wycliffe House, Water Lane, Wilmslow, Cheshire, United Kingdom SK9 5AF
Telephone:	+44 0303 123 1113
Email:	notification@ico.org.uk or informationgovernance@ico.org.uk
Website:	www.ico.org.uk

57.7 What is the scope of reporting permitted?

Reporting is permitted when, in the reasonable belief of the worker, one or more of the six specified types of malpractice has taken place, is taking place or is likely to take place and it is in the public interest to disclose this information:

- Criminal offenses;
- Breach of any legal obligation;
- Miscarriage of justice;

- Danger to the health and safety of any individual;
- Damage to the environment; and
- The deliberate concealing of information about any of the above.

57.8 Are there limits on who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

All workers receive protection from being subjected to any detriment linked as a result of them having made a protected disclosure. They have this right regardless of whether a whistleblowing policy is in place. The definition of "worker" is drafted more widely than the typical definition for a worker under U.K. law.

The whistleblowing legislation in the U.K. imposes no positive obligations on employers to encourage whistleblowing or to implement a whistleblowing policy, subject to the following requirements:

(a) Public bodies: the Government expects all public bodies to have written policies. The whistleblowing arrangements in local authorities and National Health Service bodies are assessed as part of their annual audit process.

(b) Listed companies: the Combined Code on Corporate Governance requires U.K.-listed companies to have written whistleblowing arrangements, or to explain why they do not. The company's audit committee is responsible for keeping them under review.

57.9 Are there limits on who can be a subject of a report?

No, although for a disclosure to receive protection it must relate to one of the six types of malpractice set out in the response to Question 57.7 above.

57.10 Is anonymous reporting permitted?

Yes, provided that the whistleblower policy as created allows for anonymous reporting it will be allowed. However, the Information Commissioner's Office has confirmed that its main data protection concerns arise from whistleblowing policies that encourage anonymous reporting. Where an individual is accused of wrongdoing or malpractice by an unknown informant, it may breach the data protection principle that personal data must be collected fairly.

57.11 Are there restrictions on the transfer of data in a whistleblowing program?

Yes. The transfer of any personal data will be subject to the provisions of the Data Protection Act 1998 (DPA) and in particular any personal data that is deemed to be sensitive or any transfer of such data outside the U.K. will be subject to more stringent protections. All personal data processed in the U.K. must be processed fairly and lawfully, meeting certain conditions

as set out in the DPA. There are, however, some relaxations of the legislation, for example for transfers within the EU and to recipients situated in countries that have been recognized by the EU Commission to provide for an adequate level of data protection.

The U.K. Government is currently considering a proposal to make all prescribed persons produce an annual report of protected disclosures made within a year. It is not yet clear what information or data would be required in such a report.

57.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No, there is no a strict requirement. However, the DPA may require consent to be obtained before personal data is processed about data subjects, particularly if the personal data is "sensitive personal data" as defined in the DPA (which includes information about the commission or alleged commission of an offense). Even if consent is not required, it is considered best practice to inform the accused of the allegations against them and also the identity of anyone who will receive personal data about them as a result of the investigation, unless there is a significant risk that this will prejudice the investigation.

57.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

No, not as a matter of law but there may be individual arrangements within an organization that commit an employer to do this.

57.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

There are no obligations within PIDA that require specific security or computer systems to be in place when operating a whistleblowing policy.

However, note that if any whistleblower program is adopted, the storage of any data within the U.K. will be subject to the provisions of the DPA.

For more information, contact:

Name: Mark Greenburgh
Firm: Gowling WLG
Address: 55 Colmore Row, Birmingham, B3 2AS England
Telephone: +44 870 733 0625
Email: mark.greenburgh@gowlingwlg.com
Website: www.gowlingwlg.com

58. UNITED STATES

58.1 Applicable law and/or data protection guidelines?

Legislation exists in the United States requiring certain types of companies to enact whistleblowing programs. Specifically, the Sarbanes-Oxley Act of 2002 ("SOX"), together with Securities and Exchange Commission ("SEC") and stock exchange regulations, require audit committees of companies listed on a U.S. stock exchange to establish procedures for:

- The confidential, anonymous submission by employees of that company of concerns regarding questionable accounting or auditing; and
- The receipt, retention, and treatment of complaints received by that company relating to accounting, internal accounting controls, or auditing matters.

Companies subject to SOX that fail to meet these requirements may potentially face SEC enforcement action and/or SEC civil penalties.

The United States has numerous specific whistleblower protection laws and provisions in place at both the federal and state level covering a wide variety of topics. There also exists – particularly on the federal level – legislation that seeks to encourage whistleblowers to come forward by providing monetary awards for those whose claims are successful. Some of these laws and rules also provide for sanctions against the purported whistleblower for frivolous or clearly meritless claims.

The following are a few of the key federal whistleblower statutes in the United States:

- False Claims Act (31 U.S.C. § 3729 et seq.). The False Claims Act prohibits the submission of "knowing" false claims to obtain federal funds. Whistleblowers with evidence of fraud related to government contracts and programs may bring an action known as a *qui tam* case, on behalf of the government, in order to recover the stolen funds. In compensation for the risk and effort of filing a qui tam case, the citizen whistleblower or "relator" may be awarded a portion of the funds recovered, typically between 15 and 25 percent.
- Sarbanes-Oxley Act (18 U.S.C. § 1514A). The Sarbanes-Oxley Act, also known as the Corporate and Criminal Fraud Accountability Act of 2002, protects employees of publicly traded companies, as noted above, and employees of privately owned contractors and subcontractors of public companies. Employees who believe they have suffered an adverse employment action in retaliation for protected whistleblowing activity under this statute have 180 days to file a complaint with the federal Department of Labor. Remedies available to the whistleblower include, but are not limited to, reinstatement, back pay, and special damages (such as emotional distress damages).

- Dodd–Frank Wall Street Reform and Consumer Protection Act (12 U.S.C. Section 5301 et seq.). The Dodd Frank Act amended SOX, significantly increasing the regulation of financial institutions in the United States with the goals of restoring public confidence in the financial system and avoiding future financial crises. The Dodd-Frank Act establishes an entirely new category of whistleblowers: those who give the SEC "original information". Under the program, whistleblowers are eligible to receive cash awards of 10 to 30 percent of the sanctions collected by the SEC arising from original information they reported.

- Defend Trade Secrets Act of 2016 (amending Chapter 90 of Title 18 of the United States Code). Designed primarily to provide federal jurisdiction for the theft of trade secrets, the Defend Trade Secrets Act also offers narrow whistleblower protections. Under the Act, an individual who discloses a trade secret in confidence to a government official or an attorney solely for the purpose of reporting or investigating a suspected violation of law is "immune" from civil or criminal liability for the disclosure of that trade secret under state or federal trade secret law.

58.2 Is an English translation available?

English is the de facto national language of the United States. All applicable laws and regulations are in English.

The above referenced laws may be found at:

False Claims Act: www.law.cornell.edu/uscode/text/31/3729

Sarbanes-Oxley Act: www.law.cornell.edu/uscode/text/18/1514A

Dodd-Frank Act: www.law.cornell.edu/uscode/text/12/chapter-53

Defend Trade Secrets Act of 2016, Public Law 114–153:
https://www.congress.gov/114/plaws/publ153/PLAW-114publ153.pdf

58.3 Is prior notification or approval required?

No. Companies need not seek approval from, or otherwise inform in advance, any government agency or entity prior to setting up a whistleblower program. Under SOX, however, national securities exchanges must prohibit the initial or continued listing of any security of an issuer that does not have a compliant whistleblower program in place. The United States does not have a Data Protection Authority per se, but agencies like the Federal Trade Commission (FTC), the SEC, and state Attorneys General provide guidance, and do have oversight and enforcement authority in particular discrete areas that may be relevant.

58.4 Can notification or approval be filed online?

Not applicable. See response to 58.3.

58.5 Generally, how long does it take to get approval?

Not applicable. See response to 58.3.

58.6 Contact information for Data Protection Authority?

Not applicable.

58.7 What is the scope of reporting permitted?

There exist no statutory limits on the reporting a company may allow under its corporate whistleblowing program, but there are clear subject-matter limits in particular laws, as discussed in 58.8 below. Companies in the United States have enacted a wide-range of whistleblowing programs ranging from narrow to broad, often depending upon the industry sector in which the company resides.

58.8 Are there limits as to who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

There exist no statutory limits on who a company may allow to make a report under its corporate whistleblowing program, but there are subject-matter limits in particular laws. For example, the federal False Claims Act only applies to claims of fraud against the U.S. government. The federal Sarbanes-Oxley Act only protects those who have disclosed conduct that the employee reasonably believes violates "any provision of Federal law relating to fraud against shareholders." Similarly, state and federal anti-discrimination statutes protect those who assert their rights under those statutes against retaliation from their employers. Those laws would not, however, protect the employees against retaliation for reporting on subject matter that is not covered or addressed therein (e.g., a retaliation prohibition in an anti-discrimination statute will not protect the employee against retaliation arising out of a complaint of securities fraud).

58.9 Are there limits as to who can be a subject of a report?

There are some limits on whom an employer may designate as potential subjects of reports, which depend on the statute and the company corporate whistleblowing program. See the responses to Questions 58.7 and 58.8 above.

58.10 Is anonymous reporting permitted?

Yes, anonymous reporting is permitted in a corporate whistleblowing program. In fact, the Sarbanes-Oxley Act requires that covered companies enact a mechanism for the confidential, anonymous submission by employees of concerns regarding questionable accounting or auditing practices.

58.11 Are there restrictions on the transfer of data in a whistleblowing program?

To date, the United States has no single data protection law comparable to the EU's Data Protection Directive, GDPR, EU member state data protection laws or guidelines restricting the transfer of personal data in a corporate whistleblowing program to another country. There are, however, certain computer security-related laws or regulations in the United States that may, conceivably, impact or require protections for the transfer of certain types of data used or submitted in a whistleblowing program (e.g., Social Security numbers).

58.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

No law requires that companies receive the consent of employees before establishing a whistleblower program or transferring data within it.

58.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

In unusual circumstances involving a whistleblower program that can be deemed to affect the terms and conditions of the employment of union members (for instance, whistleblowing programs that impose discipline if employees fail to report certain types of behavior), the employer may have a duty to bargain with the union over its institution. Employee consent, however, would never be required. The employer's duty would be limited to bargaining with the union in good faith over the expected effects of the program on union members.

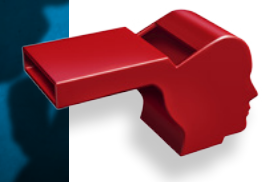
58.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

No. Material used or submitted in a whistleblowing program may, however, fall within the ambit of certain computer security-related acts governing the handling of such material (as discussed above).

For more information, contact:

Name: Mark E. Schreiber
Firm: Locke Lord LLP
Address: 111 Huntington Avenue, Boston MA 02199, USA
Telephone: +1 617 239 0585
Fax: +1 617 316 8352
Email: mark.schreiber@lockelord.com
Website: www.lockelord.com

Name: William M. Dunham
Firm: Locke Lord LLP
Address: 111 Huntington Avenue, Boston MA 02199, USA
Telephone: +1 617 239 0248
Fax: +1 866 955 8805
Email: william.dunham@lockelord.com
Website: www.lockelord.com



Name: Julie M. Engbloom
Firm: Lane Powell PC
Address: 601 SW Second Avenue, Suite 2100, Portland, OR 97204-3158, USA
Telephone: +1 503 778 2183
Fax: +1 503 778 2200
Email: engbloomj@lanepowell.com
Website: www.lanepowell.com

Name: Darin M. Sands
Firm: Lane Powell PC
Address: 601 SW Second Avenue, Suite 2100, Portland, OR 97204-3158
Telephone: +1 503 778 2117
Fax: +1 503 778 2200
Email: sandsd@lanepowell.com
Website: www.lanepowell.com

59. URUGUAY

59.1 Applicable law and/or data protection guidelines?

No. Uruguay has no specific whistleblower protection laws in place, except with respect to money laundering. However, there are labour laws, constitutional and data protection laws ("DPL") and jurisprudence that provide certain guidelines, although they do not directly address the issue.

59.2 Is an English translation available?

No.

59.3 Is prior notification or approval required?

No, it is not necessary to notify or seek approval from any agency or authority to set up a whistleblower program.

Nevertheless, if the whistleblower program includes the creation of a database with personal information related to individuals or legal entities, the company responsible for such a database (if it falls under the scope of the Uruguayan legal framework) must comply with data protection regulations, which include the duty to register the database before the Personal Data Regulatory and Control Unit "Unidad Reguladora y de Control de Datos Personales" ("DPA").

The Uruguayan regulatory framework applies if: (a) the person/company responsible for the database or for its processing is located in Uruguay; or (b) the person/company responsible for the database or for its processing is located outside Uruguay but uses for such processing, means located in Uruguay (e.g., servers hosted in Uruguay).

59.4 Can notification or approval be filed online?

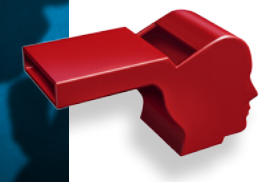
Not applicable

59.5 Generally, how long does it take to get approval?

Not applicable

59.6 Contact information for Data Protection Authority?

Name:	Unidad Reguladora y de Control de Datos Personales
Address:	Andes N° 1365, 7th floor, Montevideo, 11000, Uruguay
Telephone:	+598 2 901 0065 option 3
Email:	infocdp@agesic.gub.uy
Website:	www.datospersonales.gub.uy



59.7 What is the scope of reporting permitted?

There is no limit to the scope permitted for reporting in whistleblowing programs in Uruguay (audit, financial matters, bribery, corruption, discrimination, etc.).

59.8 Are there limits as to who can make a report under a whistleblowing program? (E.g., only managers and executives? Other employees? Suppliers?)

No.

59.9 Are there limits as to who can be a subject of a report?

No.

59.10 Is anonymous reporting permitted?

Yes, anonymous reporting is allowed and usually implemented. The company must, however, obtain the information legally and guarantee the accused employee's right to be heard.

59.11 Are there restrictions on the transfer of data in a whistleblowing program?

Personal data may only be disclosed for the purposes directly related to the legitimate interest of the issuer and the recipient, and with the prior consent of the data owner (except in cases where an exception applies and the consent is not required).

Prior consent is not required to disclose data to third parties in the following cases:

(i) It is so provided by a law of general interest;

(ii) In the cases established in section 9 of the DPL which include:

a) data arising from a public source;

b) listings containing the following limited data: in the case of individuals, the names and surnames, identity documents, nationality, address and date of birth; in the case of legal entities, name of the company, commercial name (if applicable), taxpayers' identification number, address, telephone number and identity of representatives; or

c) data arising from a contractual, scientific or professional relationship with the data subject, if such data is necessary for the performance or development of said relationship.

(iii) It is related to personal data connected to health issues and for reasons of public health and hygiene, emergency or to carry out epidemiological studies, as long as the identity of the individual is preserved through appropriate mechanisms of dissociation; or

(iv) When it is not possible to individualize anyone as part of the database because a dissociation procedure had been previously applied.

The consent of the data owner shall be prior, informed, explicit, and documented. Consent, together with other statements, shall clearly and expressly be issued upon due notice of the following information:

i) the purpose for which data shall be processed and who the recipients or class of recipients thereof shall be;

ii) the existence of the relevant database, electronic or otherwise, and the identity and address of the responsible person;

iii) the mandatory or optional nature of the answers to the questions posed, especially regarding sensitive data (if applicable);

iv) the consequences of providing data and of the refusal to do so, or of their inaccuracy (if applicable); and,

v) the possibility of the data owner to exercise the right to access, modify and delete data.

The recipient of personal data shall be subject to the same legal and regulatory obligations of the issuer who shall be jointly and severally liable for the compliance.

In addition to the above-mentioned considerations which should also be considered in cases of cross-border personal data transfers, international transfer of personal data to any country or international organization that does not provide adequate protection levels is prohibited with certain exceptions listed below:

i) International judicial cooperation and international cooperation between intelligence agencies fighting against organized crime, terrorism and drug trafficking;

ii) When the transfer is necessary for the performance or development of an agreement between the individual and the person responsible for the database;

iii) When the transfer is necessary for the execution or performance of an agreement between the person responsible for the database and a third party, signed or to be signed in the interest of the data subject;

iv) When the transfer is deemed necessary or legally required to safeguard an important public interest, or for the recognition, exercise or defense of a right in a legal procedure;

v) When the transfer is necessary for safeguarding the vital interests of the interested party; or

vi) When there is prior consent of the person to whom the data refers, etc.

The countries considered by the DPA as holding an adequate protection level are the EEA countries, as well as the non-EEA countries that according to the European Commission ensure an adequate data protection level.

Notwithstanding the prohibition referred to above, the DPA may authorize the international transfer of personal data to countries that fail to provide an adequate protection level, provided that the exporter of data offers sufficient safeguards as to the protection of privacy, rights and freedoms of individuals, and the exercise of their respective rights. Such guarantees may arise from a written agreement.

Further, if personal data is transferred to the head office of a company or any affiliated entity or branch, it may be possible to avoid obtaining the prior authorization of the DPA each time a transfer is made within such entities, if a Code of Conduct of Professional Practice which contains provisions for the processing of the information is registered before the DPA.

59.12 Is the consent of employees required for either a whistleblower program or for the transfer of data in a whistleblowing program?

Yes. Prior written consent of employees is required to: a) create a database with their personal information, unless the information incorporated in the database is needed to perform their employment activities and/or to evaluate their performance; and b) transfer the above-mentioned information to a third party, except in case an exception applies.

59.13 Is the consent of, or consultation with, a Works Council, union or other employee representative group required?

No. There is no need for consultation with a Works Council or any union or other employee representative group for the implementation of the whistleblowing programs.

59.14 Are there any specific computer or other security requirements, including the deletion of the reported information, for the whistleblower program?

Yes. The DPL provides that the person responsible or the user of the database shall take the steps necessary to guarantee the security and confidentiality of personal data. Such steps are aimed at avoiding its adulteration, loss, unauthorized processing or consultation, as well as detecting intentional or unintentional data dissociation, whether the risks result from human action or from the technical means used. Data shall be stored so that they allow the exercise of the right of access of the data holder.

Further, it is prohibited to register personal data in databases that do not meet technical requirements of integrity and security and the data collected or treated must be removed when it is no longer necessary or relevant to the purposes for which it was collected.

For more information, contact:

Name:	Diego Baldomir or Sofía Anza
Firm:	Guyer & Regules
Address.	Plaza Independencia 811, 11100 Montevideo, Uruguay
Telephone:	+598 2902 1515 int. 140 or +598 2902 1515 int. 271
Fax:	+598 2902 5454 or (598) 2902 5454 int. 7271
Email:	dbaldomir@guyer.com.uy or sanza@guyer.com.uy
Website:	www.guyer.com.uy

LIST OF CONTRIBUTORS

Argentina

Name: Pedro Mazer and Paola Trigiani
Firm: Alfaro-Abogados
Address: Avenida Del Libertador 498, Floor 3°, Buenos Aires, Argentina
Telephone: +54 11 4393 3003
Fax: +54 11 4393 3001
Email: pmazer@alfarolaw.com or ptrigiani@alfarolaw.com
Website: www.alfarolaw.com

Australia

Name: Veronica Scott and Tarryn Wood
Firm: Minter Ellison
Address: Rialto Towers, 525 Collins Street, Melbourne, VIC 3000, Australia
Telephone: +61 3 8608 2126 or +61 3 8608 2654
Fax: +61 3 8608 1181 or + 61 3 8608 1000
Email: veronica.scott@minterellison.com or tarryn.wood@minterellison.com
Website www.minterellison.com

Austria

Name: Robert Keisler and Dr. Bernt Elsner
Firm: CMS Austria
Address: Gauermanngasse 2, 1010 Vienna, Austria
Telephone: +43 1 40443/2850 or +43 1 40443/1800
Fax: +43 1 40443 9000
Email: robert.keisler@cms-rrh.com or bernt.elsner@cms-rrh.com
Website: www.cms-rrh.com

Belgium

Name: Renaud Dupont
Firm: CMS Belgium
Address: Chaussee de La Hulpe 178, B-1170 Brussels, Belgium
Telephone: +32 2 743 69 83
Fax: +32 2 743 69 01
Email: renaud.dupont@cms-db.com
Website www.cms-db.com

Brazil

Name: Renata Muzzi Gomes de Almeida
Firm: TozziniFreire Advogados
Address: Rua Borges Lagoa, 1328, Sao Paulo, SP, 04038-904, Brazil
Telephone: +55 11 5086 5000
Fax: +55 11 5086 5555
Email: rmuzzi@tozzinifreire.com.br
Website www.tozzinifreire.com.br

Bulgaria

Name: Desislava Todorova
Firm: CMS Bulgaria
Address: 4 Knyaz Alexander I Battenberg Str., fl. 2, 1000 Sofia, Bulgaria
Telephone: +359 2 447 1321
Fax: +359 2 447 1390
Email: desislava.todorova@cms-rrh.com
Website: www.cms-rrh.com

Canada

Name: Stéphane Eljarrat
Firm: Davies Ward Phillips & Vineberg LLP
Address: 1501 McGill College Avenue, 26th Floor, Montréal QC H3A 3N9, Canada
Telephone: +514 841 6439
Fax: +514 841 6499
Email: seljarrat@dwpv.com
Website: www.dwpv.com

Name: Peter Ruby
Firm: Goodmans LLP
Address: Bay Adelaide Centre, 333 Bay Street, Suite 3400, Toronto, ON, M5H 2S7, Canada
Telephone: +416 597 4184
Fax: +416 979 1234
Email: pruby@goodmans.ca
Website: www.goodmans.ca

Chile

Name: Sergio Orrego and Nicholas Mocarquer
Firm: Urenda, Rencoret, Orrego y Dörr
Address: Av. Andrés Bello 2711, 16th floor, 7550611 Las Condes, Santiago - Chile
Telephone: +562 2499 5531
Fax: +562 2499 5555
Email: sorrego@urod.cl or nmocarquer@urod.cl
Website: www.urod.cl

China, People's Republic of

Name: Gary Gao
Firm: Zhong Lun Law Firm
Address: Level 10 & 11, Two IFC, No. 8 Century Avenue, Pudong New Area, Shanghai 200120, PRC
Telephone: +86 21 60613666
Fax: +86 21 60613555
Email: gaojun@zhonglun.com
Website: www.zhonglun.com

Columbia

Name: Diego Cardona
Firm: Philippi, Prietocarrizosa &Uría
Address: Carrera 9 # 74-08, Bogota D.C., Colombia
Telephone: +571 326 8600 Ext. 1419
Fax: +571 326 8419
Email diego.cardona@ppulegal.com
Website: en.ppulegal.com

Costa Rica

Name: Valeria Agüero and Carolina Muñoz
Firm: Arias & Muñoz
Address: Costa Rica, Centro Empresarial Forum 1, Edificio C, oficina 1C1.
Telephone: +506 2503 9800
Fax: +506 2204 7580
Email: vaguero@ariaslaw.co.cr or cmunoz@ariaslaw.co.cr
Website: www.ariaslaw.com

Croatia

Name: Marija Mušec
Firm: Odvjetničko društvo Bardek, Lisac, Mušec, Skoko d.o.o. in cooperation with CMS Austria
Address: Ilica 1, 10000 Zagreb, Croatia
Telephone: +385 1 4825 600
Fax: +385 1 4825 601
Email: marija.musec@bmslegal.hr
Website: www.bmslegal.hr

Czech Republic

Name: Thomas Rechberger, Ph.D.
Firm: TaylorWessing e|n|w|c advokáti v.o.s.
Tel: +420 224 81 92 16
Email: t.rechberger@taylorwessing.com
Website: www.taylorwessing.com

Denmark

Name: Arly Carlquist and Susanne Stougaard
Firm: Bech-Bruun
Address: Langelinie Allé 35, 2100 Copenhagen, Denmark
Telephone: +45 72273462
Fax: +45 72270027
Email: ac@bechbruun.com or sus@bechbruun.com
Website: www.bechbruun.com

El Salvador

Name: Fernando Montano
Firm: Arias & Muñoz
Address: Calle La Mascota #533, Colonia San Benito. San Salvador, El Salvador
Telephone: +503 2257-0900
Fax: +503 2257-0901
Email: fernando.montano@ariaslaw.com
Website: www.ariaslaw.com

European Union

Name: Christian Runte
Frim: CMS Germany
Address: Nymphenburger Straße 12, 80335 Munich, Germany
Telephone: +49 89 23807 163
Fax: +49 89 23807 40804
Email: christian.runte@cms-hs.com
Website: www.cms-hs.com

Finland

Name: Eija Warma and Anette Luomala
Firm: Castrén & Snellman Attorneys Ltd.
Address: PO Box 233 (Eteläesplanadi 14), FI-00131, Helsinki, Finland
Telephone: +358 20 7765 376
Fax: +358 20 7761 376
Email: eija.warma@castren.fi or anette.luomala@castren.fi
Website: www.castren.fi

France

Name: Emilie Ducorps Prouvost and Laure Marolleau
Firm: Soulier Avocats
Address: 50 Avenue de Wagram, 75017 Paris, France
Telephone: + 33 (0)1 40 54 29 29
Fax: + 33 (0) 1 40 54 29 20
Email: e.ducorpsprouvost@soulier-avocats.com or l.marolleau@soulier-avocats.com
Website: www.soulier-avocats.com

Germany

Name: Christian Runte
Frim: CMS Germany
Address: Nymphenburger Straße 12, 80335 Munich, Germany
Telephone: +49 89 23807 163
Fax: +49 89 23807 40804
Email: christian.runte@cms-hs.com
Website: www.cms-hs.com

Greece

Name: Popi Papantoniou and Manto Charitos
Firm: Bahas, Gramaridis & Partners
Address: 26 Filellinon Street, Athens 105 58, Greece
Telephone: +30 210 331 8170
Fax: +30 210 331 8171
Email: p.papantoniou@bahagram.com or m.charitos@bahagram.com
Website: www.bahagram.com

Guatemala

Name: Pamela Jiménez
Firm: Arias & Muñoz
Address: Diagonal 6, 10-01 zona 10 Centro Gerencial Las Margaritas, Torre II, oficina 402-B. Ciudad de Guatemala, Guatemala, C. A.
Telephone: +502 2382 7700
Fax: +502 2382 7743
Email: pamela.jimenez@ariaslaw.com
Website: www.ariaslaw.com

Honduras

Name: René Serrano
Firm: Arias & Muñoz
Address: Centro Comercial El Dorado 6° Piso, Boulevard Morazán, Tegucigalpa, Honduras
Telephone: +504 2221 4505
Fax: +504 2221 4522
Email: rene.serrano@ariaslaw.com
Website: www.ariaslaw.com

India

Name: Bomi Daruwala
Firm: Vaish Associates Advocates
Address: 106, Peninsula Centre, Dr. S. S. Rao Road, Parel, Mumbai – 400012
Telephone: +91 22 4213 4101
Fax: +91 22 4213 4102
Email: bomi@vaishlaw.com
Website: www.vaishlaw.com

Indonesia

Name: Richard Cornwallis
Firm: Makarim & Taira S.
Address: Summitmas I, 16th & 17th floors, Jl. Jend. Sudirman Kav. 61-62, Jakarta 12190
Telephone: + 6221 252 1272, 520 0001
Fax: +6221 252 2750, 252 2751
Email: Richard.Cornwallis@makarim.com
Website: www.makarim.com

Ireland

Name: Robert McDonagh and Elizabeth Ryan
Firm: Mason Hayes & Curran
Address: South Bank House, Barrow Street, Dublin 4, Ireland
Telephone: +353 1 614 5000
Fax: +353 1 614 5001
Email: rmcdonagh@mhc.ie or eryan@mhc.ie
Website: www.mhc.ie

Israel

Name Nurit Dagan and Moria Tam-Harshoshanim
Firm: Herzog, Fox & Neeman Law Office
Address: Asia House, 4 Weizmann St, Tel Aviv 64239, Israel
Telephone: +972 3 692 7424 and +972 3 692 5530
Fax: +972 3 696 6464
Website: www.hfn.co.il
Email: dagan@hfn.co.il or tam@hfn.co.il

Italy

Name: Daniele Vecchi and Melissa Marchese
Firm: Gianni, Origoni, Grippo, Cappelli & Partners
Address: Piazza Belgioioso, 2 20121, Milan, Italy
Telephone: +39 02 7637 41
Fax: +39 02 7600 9628
Email: dvecchi@gop.it or mmarchese@gop.it
Website: www.gop.it

Japan

Name: Hitoshi Sakai
Firm: City-Yuwa Partners
Address: Marunouchi Mitsui Building, 2-2-2 Marunouchi, Chiyoda-ku, Tokyo, 100-0005
Telephone: + 81 3 6212 5642
Fax: + 81 3 6212 5700
Email: hitoshi.sakai@city-yuwa.com
Website: www.city-yuwa.com

Luxembourg

Name: Héloïse Bock
Firm: Arendt & Medernach S.A.
Address: 41A, avenue J.F. Kennedy, L-2082 Luxembourg
Telephone: +352 40 7878 321
Fax: +352 40 7804 609
Email: Heloise.Bock@arendt.com
Website: www.arendt.com

Malaysia

Name: Shanti Mogan
Firm: Shearn Delamore & Co.
Address: 7th Floor Wisma Hamzah Kwong Hing, No 1 Leboh Ampang, 50100 Kuala Lumpur, Malaysia
Telephone: +603 2027 2921
Fax: +603 2034 2763
Email: shanti@shearndelamore.com
Website: www.shearndelamore.com

Mexico

Name: César G. Cruz Ayala and Diego R. Acosta Chin
Firm: Santamarina y Steta
Address: Ricardo Margain Zozaya 335, Piso 7, Col. Valle del Campestre, 66265 San Pedro Garza García, N.L., (Monterrey) México
Telephone: +52 81 8133 6002 or +52 81 8133 6018
Fax: +52 81 8368 0111
Email: ccruz@s-s.mx or dacosta@s-s.mx
Website: www.s-s.mx/site/eng

Mongolia

Name: Elisabeth Ellis
Firm: Minter Ellison
Address: Suite 612 Central Tower, Great Chinggis Khaan's Square 2, Sukhbaatar District – 8, Ulaanbaatar, Mongolia
Telephone: +976 7700 7780
Fax: +976 7700 7781
Email: elisabeth.ellis@minterellison.com
Website: www.minterellison.com

Montenegro

Name: Milica Popović
Firm: CMS Montenegro
Address: Bulevar Džordža Vašingtona 3/22, 81000 Podgorica, Montenegro
Telephone: +382 20 416 070 / +381 11 320 8900
Fax: +382 20 416 071
Email: milica.popovic@cms-rrh.com
Website: www.cms-rrh.com

Mozambique

Name: Tomás Timbane
Firm: TTA Sociedade de Avogados
Address: Edifício Millennium Park, Torre A, Avenida Vladimir Lenine, nº 179, 6º Dtº, Maputo – Moçambique
Telephone: +258 843 141 820
Email: tomas.timbane@tta-advogados.com
Website: www.tta-advogados.com

Name: Miguel Spinola
Firm: PLMJ Sociedade de Advogados, RL
Address: Edifício Eurolex, Avenida da Liberdade, 224, 1250-148 Lisbon - Portugal
Telephone: +351 213 197 446
Mobile: +351 916 346 219 or +258 843 318 695
Fax: +351 21 319 74 00
Email: miguel.spinola@plmj.pt
Website: www.plmj.com

The Netherlands

Name: Hendrik Struik
Firm: CMS Netherlands
Address: Newtonlaan 203, 3584 BH Utrecht, The Netherlands
Telephone: +31 30 212 1726
Fax: +31 30 212 1157
Email: hendrik.struik@cms-dsb.com
Website: www.cms-dsb.com

New Zealand

Name: Richard Wells
Firm: Minter Ellison Rudd Watts Lawyers
Address: Lumley Centre, 88 Shortland Street, Auckland 1010, New Zealand
Telephone: +64 9 353 9908
Fax: +64 9 353 9701
Email: richard.wells@minterellison.co.nz
Website: www.minterellison.co.nz

Nicaragua

Name: Roberto Argüello
Firm: Arias & Muñoz
Address: Pista Jean Paul Genie, Edificio Escala, 3er piso, Managua, Nicaragua
Telephone: +505 2298 1360
Email: roberto.arguello@ariaslaw.com
Website: www.ariaslaw.com

Norway

Name: Kaare Risung and Trond Stang
Firm: Advokatfirmaet Schjødt AS
Address: Ruseløkkveien 14, P.O. Box 2444 Solli, NO-0201 Oslo, Norway
Telephone: +47 23 01 18 00
Fax: +47 22 83 1712
Email: kmr@schjodt.no or trst@schjodt.no
Website: www.schjodt.no

Panama

Name: Siaska Lorenzo, Partner
Firm: Arias & Muñoz
Address: Torre Global, Piso 23, Oficina 2305, Calle 50, Panama City, Panama
Telephone: +507 282 1400
Fax: +507 282 1435
Email: siaska.lorenzo@ariaslaw.com
Website: www.ariaslaw.com

Peru

Name: Carlos A. Patron and Giancarlo Baella
Firm: Payet Rey Cauvi Perez Abogados
Address: Av. Victor Andres Belaunde 147, Centro Empresarial Real, Torre Real Tres Piso 12, San Isidro, Lima 27, Perú
Telephone: +511 612 3202
Fax: +511 222 1573
Email: cap@prc.com.pe or gbp@prc.com.pe
Website: www.prc.com.pe

Philippines

Name: Rolando V. Medalla, Jr. or Hiyasmin H. Lapitan or Azyleah V. Ignacio and Patricia A. Madarang
Firm: SyCip Salazar Hernandez & Gatmaitan
Address: SyCipLaw Center, 105 Paseo de Roxas, Makati City 1226, The Philippines
Telephone: +63 2 982 3500 or +63 2 982 3600, or +63 2 982 3700
Fax: +63 2 817 3145 or +63 2 817 3896
Email: rvmedalla@syciplaw.com or hhlapitan@syciplaw.com or avignacio@syciplaw.com or pamadarang@syciplaw.com
Website: www.syciplaw.com

Poland

Name: Agata Szeliga and Katarzyna Paziewska
Firm: Sołtysiński Kawecki & Szlęzak
Address: ul. Jasna 26, 00-054 Warszawa, Poland
Telephone: +48 22 608 7006 or +48 22 608 7190
Fax: +48 22 608 7070
Email: agata.szeliga@skslegal.pl or katarzyna.paziewska@skslegal.pl
Website: www.skslegal.pl

Portugal

Name: Daniel Reis and Marta Costa
Firm: PLMJ – Sociedade de Advogados, RL
Address: Lisboa Av. da Liberdade, 224, Edifício Eurolex, 1250-148 Lisboa, Portugal
Telephone: +351 21 319 7300 or direct dial +351 21 319 7313
Fax: 351 21 319 7400
Email: daniel.reis@plmj.pt or marta.costa@plmj.pt
Website: www.plmj.pt

Russia

Name: Anton Bankovskiy and Vladislav Eltovskiy
Firm: CMS Russia
Address: Presnenskaya nab. 10, 123317 Moscow, Russia
Telephone: +7 49 5786 4000
Fax: +7 49 5786 4001
Email: Anton.Bankovskiy@cmslegal.ru Vladislav.Eltovskiy@cmslegal.ru
Website: www.cmslegal.ru

Serbia

Name: Radivoje Petrikić and Ksenija Ivetić Marlović
Firm: Petrikić & Partneri AOD in cooperation with CMS Austria
Address: Cincar Jankova 3, 11000 Belgrade, Serbia
Telephone: +381 11 320 8900
Fax: +381 11 303 8930
Email: radivoje.petrikic@cms-rrh.com or ksenija.ivetic@cms-rrh.com
Website: www.cms-rrh.com

Slovakia

Name: Michal Kohn
Firm: Ruži ka Csekes, in association with CMS Austria
Address: Vysoká 2/B, 811 06 Bratislava, Slovakia
Telephone: +421 2 3233 3444
Fax: +421 2 3233 3443
Email: michal.kohn@rc-cms.sk
Website: www.rc-cms.sk

Slovenia

Name: Luka Fabiani
Firm: CMS Slovenia
Address: Bleiweisova 30, SI-1000 Ljubljana, Slovenia
Telephone: +386 1 6205 210
Fax: +386 1 6205 211
Email: luka.fabiani@cms-rrh.com
Website: www.cms-rrh.com

South Africa

Name: Dave Loxton
Firm: ENSafrica
Address: 150 West Street, Sandton, Johannesburg, South Africa 2196
Telephone: +27 11 269-7600
Fax: +27 11 269 7899
Email: dloxton@ensafrica.com
Website: www.ensafrica.com

South Korea

Name: Taeuk Kang
Firm: Bae, Kim and Lee LLC
Address: Hyundai Marine & Fire Insurance Bldg. 17F, 137 Teheranro, Gangnamgu, Seoul
Telephone: +82 2 3404 0485
Fax: +82 2 3404 0001
Email: taeuk.kang@bkl.co.kr
Website: www.bkl.co.kr

Spain

Name: Jorge Llevat and Jorge Monclús
Firm: Cuatrecasas, Gonçalves Pereira
Address: Paseo de Gracia 111, 08008 Barcelona, Spain
Telephone: +34 93 2905 585
Fax: +34 93 2905 569
Email: jorge.llevat@cuatrecasas.com or jorge.monclus@cuatrecasas.com
Website: www.cuatrecasas.com

Sweden

Name: Fredrik Roos and Bobi Mitrovic
Firm: Setterwalls Advokatbyrå AB
Address: Sankt Eriksgatan 5, P.O. Box 11235, SE-404 25, Gothenburg, Sweden
Telephone: +46 31 701 1700
Fax: +46 31 701 1701
Email: fredrik.roos@setterwalls.se or bobi.mitrovic@setterwalls.se
Website: www.setterwalls.se

Switzerland

Name. Dr. Robert G. Briner,
Firm: CMS Switzerland
Address: Dreikönigstrasse 7, 8002 Zurich, Switzerland
Telephone: +41 44 285 1111
Fax: +41 44 285 1122
Email: robert.briner@cms-veh.com
Website: www.cms-veh.com

Taiwan

Name: Chun-yih Cheng
Firm: Formosa Transnational Attorneys at Law
Address: 13th Floor, Lotus Building, 136 Jen Ai Road Section 3, Taipei 10657, Taiwan
Telephone: +886 2 2755 7366
Fax: +886 2 2708 6035
Email: chun-yih.cheng@taiwanlaw.com
Website: www.taiwanlaw.com

Thailand

Name: Niwes Phancharoenworakul and Christopher Kalis
Firm: Chandler & Thong-ek Law Offices
Address: 7th-9th Fl., Bubhajit Building, 20 North Sathorn Rd, Bangkok 10500, Thailand
Telephone: +662 266-6485 thru 6510
Fax: +662 266-6483, 266-6484
Email: niwes@ctlo.com, or chris@ctlo.com

Turkey

Name: Kemal Mamak and Kayra Üçer
Firm: Hergüner Bilgen Özeke Attorney Partnership
Address: Büyükdere Caddesi 199, Levent 34394, Istanbul, Turkey
Telephone: +90 212 310 1800
Fax: +90 212 310 1899
Email: kmamak@herguner.av.tr or kucer@herguner.av.tr
Website: www.herguner.av.tr

Ukraine

Name: Maria Orlyk and Kateryna Soroka
Firm: CMS Ukraine
Address: 19-B Instytutska, 5th Floor, 01021 Kyiv, Ukraine
Telephone: +380 44 500 1710 or +380 44 500 1711
Fax: 380 44 500 1716
Email: maria.orlyk@cms-rrh.com or kateryna.soroka@cms-rrh.com
Website: www.cms-rrh.com

United Kingdom

Name: Mark Greenburgh
Firm: Gowling WLG
Address: 55 Colmore Row, Birmingham, B3 2AS England
Telephone: +44 870 733 0625
Email: mark.greenburgh@gowlingwlg.com
Website: www.gowlingwlg.com

United States

Name:	Mark E. Schreiber
Firm:	Locke Lord LLP
Address:	111 Huntington Avenue, Boston MA 02199, USA
Telephone:	+1 617 239 0585
Fax:	+1 617 316 8352
Email:	mark.schreiber@lockelord.com
Website:	www.lockelord.com

Name:	William M. Dunham
Firm:	Locke Lord LLP
Address:	111 Huntington Avenue, Boston MA 02199, USA
Telephone:	+1 617 239 0248
Fax:	+1 866 955 8805
Email:	william.dunham@lockelord.com
Website:	www.lockelord.com

Name:	Julie M. Engbloom
Firm:	Lane Powell PC
Address:	601 SW Second Avenue, Suite 2100, Portland, OR 97204-3158, USA
Telephone:	+1 503 778 2183
Fax:	+1 503 778 2200
Email:	engbloomj@lanepowell.com
Website:	www.lanepowell.com

Name:	Darin M. Sands
Firm:	Lane Powell PC
Address:	601 SW Second Avenue, Suite 2100, Portland, OR 97204-3158
Telephone:	+1 503 778 2117
Fax:	+1 503 778 2200
Email:	sandsd@lanepowell.com
Website:	www.lanepowell.com

Uruguay

Name:	Diego Baldomir and Sofía Anza
Firm:	Guyer & Regules
Address.	Plaza Independencia 811, 11100 Montevideo, Uruguay
Telephone:	+598 2902 1515 int. 140 or +598 2902 1515 int. 271
Fax:	+598 2902 5454 or (598) 2902 5454 int. 7271
Email:	dbaldomir@guyer.com.uy or sanza@guyer.com.uy
Website:	www.guyer.com.uy