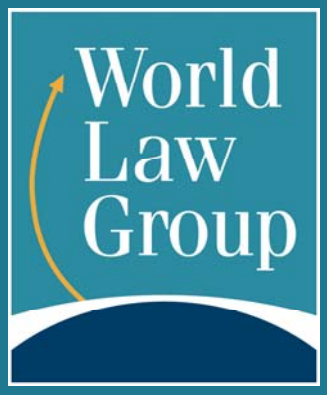

Global Guide to Whistleblowing Programs

2012

World Law Group
Global Guide to
Whistleblowing Programs

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. Local legal counsel and advice should routinely be obtained. For additional information or advice in a particular jurisdiction, you may contact the members of the World Law Group's Privacy Matters Practice Group as listed in the "Contacts" section.

CONTENTS

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.

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, was 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 proposed new EU data protection regulation will simplify this process, remains to be seen.

We have tried, with the help of numerous World Law Group firms, to point out relevant aspects of whistleblowing schemes in a substantial number of jurisdictions. Members of the WLG Privacy Matters Group have contributed to provide this information in a basic question-and-answer format. It has nevertheless been a project some time in the making. We trust it will be a valuable resource for organizations planning to establish or review whistleblowing schemes and related compliance structures.

The WLG Privacy Matters Group especially wants to thank attorney Eija Warma and her colleagues at Castrén & Snellman in Finland, as well as Inês Sà formerly with Cuatrecasas, Gonçalves Pereira in Portugal, for reviewing and helping finalize this publication. They worked tirelessly to edit the submissions from the member firms involved, and to identify and resolve the many nuances in responses from WLG lawyers around the globe.

Mark E. Schreiber, Chair, WLG Privacy Matters Group, Edwards Wildman Palmer LLP, Boston
Christian Runte, Co-Chair, WLG Privacy Matters Group, CMS Hasche Sigle, Munich

ABOUT THE WORLD LAW GROUP

The World Law Group is a network of 50 leading independent law firms with more than 275 offices in major commercial centres worldwide. WLG member firms comprise more than 15,000 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 full list of all member firms of the World Law Group and their respective 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 Matters Group

The World Law Group's Privacy Matters Practice Group is made up of lawyers in the WLG's 50 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 in cross-border data transfers, privacy risk assessment 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 collaborated to produce, for example, a seminal chapter on "Anonymous Sarbanes-Oxley Hotlines for Multinational Companies: Compliance with E.U. Data Protection Laws", for the American Bar Association's *The Practitioner's Guide to the Sarbanes-Oxley Act*, (2009), one of the leading works in this area. The Group also intends to release a multi-country reference on data breach notification requirements.

For more information, contact:

Mark E. Schreiber
Chair, WLG Privacy Matters Group
Edwards Wildman Palmer LLP
Boston, Massachusetts, U.S.A.
Email: mschreiber@edwardswildman.com
Tel: + 1 617 239 0585

Christian Runte
Co-Chair, WLG Privacy Matters Group
CMS Hasche Sigle
Munich, Germany
Email: christian.runte@cms-hs.com
Tel: + 49 89 238 07 0

ARGENTINA

1. Applicable law and/or data protection guidelines?

No. Argentina has no specific whistleblower protection laws in place. 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.

2. Is an English translation available?

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

www.privacyinternational.org/countries/argentina/argentine-dpa.html

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.

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

4. Can notification or approval be filed online?

Not applicable (N/A)

5. Generally, how long does it take to get approval?

N/A

6. Contact information for Data Protection Authority?

National Directorate for Personal Data Protection (DNPDP)
Sarmiento 1118 – 5º Piso; Ciudad Autónoma de Buenos Aires;
Buenos Aires, Argentina C1041AAX

T: +54 11 4383-8512 / 8510 / 8513 / 8514 / 8521
E: infodnpdp@jus.gov.ar
W: www.jus.gov.ar/datos-personales.aspx

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 employment.

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.

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

No.

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.

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

Yes. 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.

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 of data shall not apply in certain cases. Among the most common exceptions are:

a) The data's owner gives his express consent (the consent will not be necessary in case 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 such information to prevent the identification of the persons;

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

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 and b) transfer the above-mentioned information to a third party.

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.

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

Yes. The DPL and its Regulatory Decree 1558/2001 both 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 as 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:

Alfaro-Abogados
W: www.alfarolaw.com

Soledad Matteozzi
E: smatteozzi@alfarolaw.com

Pedro Mazer
E: pmazer@alfarolaw.com

AUSTRALIA

1. Applicable law and/or data protection guidelines?

Yes. 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.

While there is currently no equivalent statute at the Commonwealth level to protect Commonwealth public servants, provisions in other legislation afford some protection to whistleblowers on the basis of their employment. [2]

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, the fact that only four whistleblowers

1 *Public Interest Disclosure Act 1994* (ACT); *Protected Disclosures Act 1994* (NSW);*Public Interest Disclosure Act 2008* (NT); *Whistleblowers Protection Act 1994* (QLD); *Whistleblowers Protection Act 1993* (SA); *Public Interest Disclosures Act 2002* (TAS); *Whistleblowers Protection Act 2001* (VIC); and *Public Interest Disclosure Act 1994* (WA).

[2] In its "Report on the Inquiry into Whistleblowing Protection within the Australian Government Public Sector", the House of Representatives Standing Committee on Legal and Constitutional Affairs recommended that "public official" be defined in the bill to include: Australian Government and general government sector employees; contractors and consultants engaged by the public sector (as well as their employees); Australian and locally engaged staff working overseas; members of Australian Defence Force and AFP; parliamentary staff; former employees in any of the above categories as well as anonymous persons in any of the above categories.

have relied on them to provide information to ASIC as of October 2009 suggests that this framework may be in need of reform.[3]

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. Is an English translation available?

The primary language is English.

3. Is prior notification or approval required?

No. Neither public bodies nor corporations need to notify the Federal Privacy Commissioner (or other data protection authority) before setting up a whistleblower program. [4]

4. Can notification or approval be filed online?

N/A

5. Generally, how long does it take to get approval?

N/A

6. Contact information for Data Protection Authority?

Office of the Australian Information Commissioner
GPO Box 2999
Canberra, ACT 2601, Australia

T: + 61 2 9284 9749
F: + 61 2 9284 9666
E: enquiries@oaic.gov.au
W: www.oaic.gov.au

7. What is the scope of reporting permitted?
In order to be protected under the *Corporations Act 2001 (Cth)*, a whistleblower must have

[3] Media release by the Hon Chris Bowen MP, Minister for Financial Services, Superannuation and Corporate Law on 22 October 2009.
[4] See e.g. Ombudsman's Guidelines under the *Whistleblower Protection Act 2001* (Vic) accessible at: http://www.ombudsman.vic.gov.au/resources/documents/Whistleblowers_Protection_Act_2001_Ombudsmans_Guidelines4.pdf .

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.

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 offence).

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. 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 authorised deposit-taking institutition, a general insurer, or 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.

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.

10. Is anonymous reporting permitted?

No. Anonymous reporting is not permitted in the corporate sector. In some State jurisdictions, such as Victoria and Queensland, public interest disclosures can be made anonymously.

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 offence 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 protection to whistleblower information as it would to any other piece of personal information.

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).

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

No.

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:

Minter Ellison
W: www.minterellison.com

Charles Alexander
E: charles.alexander@minterellison.com

Gemma-Jane Cooper
E: gemma-jane.cooper@minterellison.com

AUSTRIA

1. Applicable law and/or data protection guidelines?

No. Austria has no specific whistleblower protection laws in place.

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

2. Is an English translation available?

Yes. An unofficial translation of the *Federal Act Concerning the Protection of Personal Data* is available: http://www.dsk.gv.at/site/6274/default.aspx

3. Is prior notification or approval required?

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

4. Can notification or approval be filed online?

No. All necessary documentation can be found on the DPA's website at www.dsk.gv.at/site/6296/default.aspx . The DPA suggests making notifications via e-mail using the forms provided online.

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 activities, and sensitive data may be started without awaiting the approval two months after notification unless the data protection commission objects to the early start.

6. Contact information for Data Protection Authority?

Geschäftsstelle der Datenschutzkommission
Hohenstaufengasse 3
1010 Wien
Vienna, Austria

T: +43 1 531 15 / 2525
F: +43 1 531 15 / 2690
E: dsk@dsk.gv.at
W: http://www.dsk.gv.at

7. What is the scope of reporting permitted?

The data protection commission 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 grievances concerning accounting, corruption and financial crime rate.

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 the employees are entitled to report. It is unclear if the external suppliers may also report under a whistleblowing program.

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

Yes. The legislation itself does not restrain the circle of persons who can be subject of a report. However, the WP 117 Art 29 Data Protection Group recommends confining the circle of persons who can be subject of a report on the principles of proportionality. The Data Protection Commission takes a narrower view in line with WP 117 Art 29 and has only approved the transfer of data to non-EEA members under the condition that only the management may be subject of a report in the whistleblowing program.

10. Is anonymous reporting permitted?

Yes, although anonymous reporting is not encouraged.

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 severe cases.

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

No.

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

Yes. Implementation requires a Works Council's approval.

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

Yes. The data protection commission requires a set of conditions to be met. Amongst others, all information reported has to be deleted at the latest two months after the finalisation of the examination.

For more information, contact:

CMS Reich-Rohrwig Hainz Rechtsanwälte GmbH
W: www.cms-rrh.com

Bernt Elsner
E: bernt.elsner@cms-rrh.com

Robert Keisler
E: robert.keisler@cms-rrh.com

BELGIUM

1. Applicable law and/or data protection guidelines?

A whistleblower program has to comply with the provisions of the Belgian *Act of 8 December 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 the *Directive 95/46/EC of the European Parliament and of the Council of 24 October 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 nr 01/2006 of 29 November 2006 regarding the compatibility of whistleblowing with Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data* (hereafter the "Recommendation of the CPP")

The Recommendation of the CPP gives 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: the *Opinion 1/2006* provided by the Article 29 Data Protection Working Party *on the application of EU data protection rules to internal whistle blowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against 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.

2. Is an English translation available?

Yes. See www.privacycommission.be

3. Is prior notification or approval required?

Yes, DPA notification is needed.

4. Can notification or approval be filed online?

Yes.

5. Generally, how long does it take to get approval?

Usually less than three months.

6. Contact information for Data Protection Authority?

Belgian Commission for the Protection of Privacy
139, rue Haute
1000 Brussels

T: +32 (0)2 213 85 40
F: +32 (0)2 213 85 65
E: commission@privacycommission.be
W: www.privacycommission.be

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.[5]

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

- A legal or regulatory provision imposing the company to process personal data through such systems, 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 as a valid "legal or regulatory provision (...)" but can constitute the "legitimate interest".

[5] 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 by 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.

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

The Recommendation of the CPP 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,
- be able to act with sufficient independence,
- be subject to liability in case of breach of the confidentiality,
- be protected from pressure from his/her hierarchy or professional organisations.

The whistle blower 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,
- 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 shall assure that the outsourcing service comply with the aforementioned requirements.

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

No.

10. Is anonymous reporting permitted?

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

Anonymous reports are exceptionally allowed in so far as:

- the 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.
- the scheme informs the whistleblower that his/her identity will be kept confidential at all the stages of the process.

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 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 shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and 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.

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 want to put in place.

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.

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:

CMS DeBacker
W: www.cms-db.com

Veerle Raus
E: veerle.raus@cms-db.com

CANADA

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 of offences 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.

2. Is an English translation available?

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

3. Is prior notification or approval required?

National Instrument 52-510 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.

4. Can notification or approval be filed online?

N/A

5. Generally, how long does it take to get approval?

N/A

6. Contact information for Data Protection Authority?

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

i) investigating complaints, conducting audits and pursuing court actions under certain federal laws,

ii) publicly reporting on the personal information-handling practices of public and private sector organizations,

iii) supporting, undertaking and publishing research into privacy issues, and

iv) promoting awareness and understanding of privacy issues.

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

Office of the Privacy Commissioner of Canada
112 Kent Street
Place de Ville
Tower B, 3rd Floor
Ottawa, Ontario K1A 1H3

T: +1 613 995-2042
W: www.priv.gc.ca.

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 where the employee has reported an offence 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".

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.

9. Are there limits as to who can be 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 offence 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.

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.

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

Regarding privacy laws in Canada, the provinces of Québec, British Columbia and Alberta are the only jurisdictions to have enacted comprehensive privacy laws applicable to the private sector. The federal *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 ("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 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 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 to communicate 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 cannot give access to personal information if: 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 was 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 an individual where disclosure of the information would be likely to hinder an inquiry, the purpose of which is the prevention, detection or repression of statutory offences conducted by his internal security service or conducted on his behalf by an external. With regards to whistleblowers, section 40 provides that an organization must refuse to give communication of 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 the disclosure may seriously harm that third person.

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

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 US Patriot Act.

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

No.

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:

Davies Ward Phillips & Vineberg LLP
www.dwpv.com

Stéphane Eljarrat
E: seljarrat@dwpv.com

Goodmans LLP
www.goodmans.ca

Peter Ruby
E: pruby@goodmans.ca

CHILE

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*.

2. Is an English translation available?

No.

3. Is prior notification or approval required?

No.

4. Can notification or approval be filed online?

N/A

5. Generally, how long does it take to get approval?

N/A

6. Contact information for Data Protection Authority?

There is currently no Data Protection Authority in Chile.

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

No.

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

No.

10. Is anonymous reporting permitted?

Yes.

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 authorised 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 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, which 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 authorisation is granted by a 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, article 154 bis of the *Labour Code* provides that the employer shall maintain confidentiality of all private information and data regarding employees, which is obtained during the employment relationship

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.

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

No.

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:

Urenda, Rencoret, Orrego y Dörr
W: www.urod.cl

Ignacio Barón
E: ibaron@urod.cl

Nicholas Mocarquer
E: nmocarquer@urod.cl

CZECH REPUBLIC

1. Applicable law and/or data protection guidelines?

No. The Czech Republic has no specific whistleblower protection laws in place.

The Czech *Personal Data Protection Act* ("PDPA") relies on the principles enshrined in *Act No. 101/2000 Coll., on the Protection of Personal Data*, which can be found at http://www.uoou.cz/uoou.aspx?menu=4&submenu=5&loc=20, and 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, fight against bribery, banking and financial crime (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_en.pdf).

2. Is an English translation available?

A Consolidated version of the *Personal Data Protection Act* and on related amendments to other Acts is available in English. (But please note that the translation does not reflect several recent amendments to the PDPA). See http://www.uoou.cz/uoou.aspx?menu=4&submenu=5&lang=en.

3. Is prior notification or approval required?

Yes. A notification to the DPA is needed when a whistleblowing program is likely to involve processing of personal data that does not fall under the statutory exemptions (such as fulfilment of a legal obligation by the controller or the protection of his legitimate interests).

4. Can notification or approval be filed online?

Yes. There is an online form.

5. Generally, how long does it take to get approval?

The DPA must, within 30 days from the submission of the notification, request further information or clarifications in relation to the notification. If it does not act, then after the 30-day period, the notification is 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.

6. Contact information for Data Protection Authority?

Úřad pro ochranu osobních údajů
Pplk. Sochora 27
170 00 Praha 7
Prague, Czech Republic

T: (Information) +420 234 665 555
T: (Switchboard) +420 234 665 111
F: +420 234 665 444
E: posta@uoou.cz
W: www.uoou.cz

7. What is the scope of reporting permitted?

There is no defined scope of reporting.

However, reporting must be strictly adequate to the purpose and therefore, for instance, reporting sensitive personal data, including sexual orientation, ethnic or social origin, trade union or political membership or religion would not likely be approved.

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

No.

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

No.

10. Is anonymous reporting permitted?

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

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

No. Only general rules implementing data transfer provisions of the Directive apply (e.g., transfer to a Safe Harbour certified entity does not need to be approved by the DPA).

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

No.

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 scheme.

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 scheme, including the periods for which the personal data may be retained, must be strictly adequate to the purpose of processing. Although there are no specific data retention periods prescribed by the law (except for the general "shortest-as-possible" requirement), the scheme must specify for how long the data will be retained and justify those periods.

For more information, contact:

Havel, Holásek & Partners s.r.o.
W: www.havelholasek.cz

Robert Nešpůrek
E: robert.nespurek@havelholasek.cz

Richard Ötevrel
E: richard.otevrel@havelholasek.cz

DENMARK

1. Applicable law and/or data protection guidelines?

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

However, 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 Article 29 Working Party, including WP 117/2006 concerning whistleblowing schemes.

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/

Whistleblowing guidelines:
www.datatilsynet.dk/english/whistleblower-systems/whistleblower-guidelines/

3. Is prior notification or approval required?

Yes. Both notification and authorisation 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 authorisation has been obtained. There is a filing fee DKK of 1,000, which is invoiced separately.

Additional notifications and authorisations 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 authorisation is subject to a fee.

4. Can notification or approval be filed online?

Yes. Notification and a request for authorisation can be filed online. A specific application form for private companies must be employed. The form is only available in Danish at: www.datatilsynet.dk/blanketter/anmeldelsesblanketter/privat-virksomhed/.

Please note that the application must be submitted in Danish.

5. Generally, how long does it take to get approval?

The DPA aims to process applications within five months.

6. Contact information for Data Protection Authority?

The Danish Data Protection Agency
Borgergade 28, 5
1300 Copenhagen, Denmark

T: + 45 33 19 32 00
F: + 45 33 19 32 18
E: dt@datatilsynet.dk
W: www.datatilsynet.dk

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.

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.

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.

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.

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 authorisation 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 APPD 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 – non-EU/EEA), a data processing agreement must be concluded between the data controller and the data processor.

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 APPD 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.

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. 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 unauthorised disclosure, abuse or other processing in violation of the provisions laid down in the APPD. 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 authorisation issued by the DPA with respect to the whistleblower program, the DPA will lay down the requirements for security measures which 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, *inter alia*, the following security measures:

- login and password procedures are in place,
- firewall and antivirus software is up-to-date,

- only persons with authorised access 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,
- specific logging requirements,
- persons who have authorised 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 authorised 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 APPD, 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:

Bech-Bruun
W: www.bechbruun.com

Arly Carlquist,
E: ac@bechbruun.com

Birgitte Toxværd,
E: bit@bechbruun.com

FINLAND

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 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 the system.

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/haku.php?search%5Btype%5D=pika&search%5Bpika%5D=henkil%C3%B6tietolaki

The *Act on Protection of Privacy in Working Life*:
www.finlex.fi/fi/laki/kaannokset/haku.php?search%5Btype%5D=pika&search%5Bpika%5D=laki+yksityisyyden+suojasta+ty%C3%B6el%C3%A4m%C3%A4ss%C3%A4

3. Is prior notification or approval required?

No. However, there might be an obligation to notify the DPA (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.

4. Can notification or approval be filed online?

A notification can be sent by email but there is no online filing possibility.

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 an answer from the DPA and sometimes even longer. This would not prevent a data controller from implementing a whistleblowing program.

6. Contact information for Data Protection Authority?

Tietosuojavaltuutetun toimisto
PL 315
00181 Helsinki, Finland

T: +358 (0)10 36 66700
E: tietosuoja@om.fi
W: www.tietosuoja.fi/1560.htm

7. What is the scope of reporting permitted?

The scope is limited to financial matters only (such as accounting, internal accounting controls, auditing matters, bribery, banking and financial crime). Any other type of matter should be handled through Human Resources and/or a manager.

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 and it does not include external suppliers.

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

No. All employees, managers and executives can be subject to a reporting.

10. Is anonymous reporting permitted?

This is unclear under Finnish law.

A person has a right to be informed about the source of information which excludes a possibility of anonymous reporting. However, there is no statute that would specifically prohibit anonymous reporting. The DPA recommends that anonymous reporting not be used.

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.

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

No.

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 in a cooperation procedure. If a company has less than 30 employees, a 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 a 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.

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:

Castrén & Snellman Attorneys Ltd.
W: www.castren.fi

Ms. Eija Warma
E: eija.warma@castren.fi

FRANCE

1. Applicable law and/or data protection guidelines?

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

When the 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 Authorisation AU-004) authorising 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/en-savoir-plus/deliberations/deliberation/delib/83/.

2. Is an English translation available?

Yes. An official translation is available: www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf

The November 2005 guidelines on the implementation of whistleblowing programs in compliance with the French *Data Protection Act* may be found at: www.cnil.fr/fileadmin/documents/en/CNIL-recommandations-whistleblowing-VA.pdf

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 Authorisation AU-004 (simplified declaration process) if the company wishes to implement a whistleblowing program that match the requirements set forth in the Single Authorisation, or

- Apply for prior approval (standard authorisation process) if the company wishes to implement a whistleblowing program that does not precisely match these requirements.

4. Can notification or approval be filed online?

Yes.

5. Generally, how long does it take to get approval?

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

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

6. Contact information for Data Protection Authority?

Commission nationale de l'informatique et des libertés
8, rue Vivienne
CS 30223
75083 Paris cedex 02, France

T: +33 (0)1 53 73 22 22
W: www.cnil.fr/

7. What is the scope of reporting permitted?

The whistleblowing programs that are permitted under the Single Authorisation from the CNIL are the ones limited in scope to facts regarding:

a) Legal obligations of French law in relation to implementing internal audit in the fields of finance, accounting, banking, anti-corruption and now anti-competitive practices, *or*

b) Legal requirements derived from the U.S. *Sarbanes-Oxley Act* ("SOX) or the Japanese *Financial Instrument and Exchange Law* dated 6 June 2006 ("the Japanese SOX").

Whistleblowing programs not limited to this scope (e.g., those that include intellectual property or discrimination concerns, 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.

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 of the Single Authorisation, the CNIL defines whistleblowing programs as systems made available to employees. The whistleblowing programs have to define who is entitled to make a report.

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 programs.

10. Is anonymous reporting permitted?

Yes. Anonymous reporting is allowed as long as it is not actively encouraged by the company.

As a result, an individual's identification should be requested prior to reporting, but the whistleblower's identity must be kept confidential.

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 (known as "cil") and the legal framework of the transfer.

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

- The legal entity within which the recipient of the personal data works has adhered to the Safe Harbour Act; or

- 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 Authorisation requirements, this also serves as authorisation to transfer data.

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

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

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 (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*).

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 alert. In that case, data must be deleted at the end of the procedure/proceedings.

For more information, contact:

Soulier
W: www.soulier-avocats.com

Emilie Ducorps-Prouvost
E: e.ducorpsprouvost@soulier-avocats.com

Laure Marolleau
E: l.marolleau@soulier-avocats.com

GERMANY

1. Applicable law and/or data protection guidelines?

No. Germany has no specific whistleblower protection laws in place.

A. The Federal Data Protection Act as Applicable Law

There are general legal restrictions concerning data protection in Germany (*Federal Data Protection Act*, transferring the *Data Protection Directive EC 95/46*). Each company that wants to implement a whistleblower program has to comply with this Act as personal data is collected and processed during the use of a whistleblower system.

One of the main principles of the *Federal Data Protection Act* is that data collecting and processing has to be considered necessary for the performance of employment according to Section 32 of the Act, e.g., to disclose criminal action. Companies can give reasons for their legitimate interest in implementing a whistleblower programs for the prevention of fraud, bribery or serious misconduct regarding auditing or insider dealing. The whistleblower system and the personal data processed have to comply with the principle of proportionality. The respective interests of the employees are weighted against the legitimate interests of the company. Each report within a whistleblower system must comply with these principles.

Besides this, there is an obligation to notify each employee via the company's Intranet or by sending a newsletter before starting the whistleblower program. Each person involved in a whistleblower case has the right of access to his/her personal data according to Section 34 of the *Federal Data Protection Act*.

B. The Düsseldorf Group

In Germany, legislative and administrative competence in data protection issues rests with the regional state level and not within the federal realm. The Düsseldorf Group is an association of data protection authorities of the German regional states which monitors compliance of data protection in the private sector in Germany. It aims to ensure uniform application of the Federal Data Protection Act and gives recommendations.

The Düsseldorf Group defined in greater detail the legal principle of proportionality, *inter alia*, by limiting the scope of reporting to serious misconducts and frauds.

The Düsseldorf Group recommends a review of the channel by the company data protection officer with respect to automatic data processing.

Furthermore, companies should use a neutral independent party, specialised companies or law firms to operate an external whistleblower hotline. This can 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.

These external providers will also have to comply with the *Federal Data Protection Act*. They shall ensure, by means of a contract, that they collect and process personal data in accordance with the principles of data protection. In particular, they shall abide by strict confidentiality obligations and communicate the information processed only to specified persons in the company or the organization responsible for the investigation or for taking the required measures to follow up the facts reported.

C. The EU Art. 29 Working Party

The National Data Protection Authorities of the EU Member States align their policies and administrative processes in the Article 29 Working Party. The Party acts by giving opinions and coordinating international issues.

The recommendations of both the Düsseldorf Group and the EU Art. 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 *Federal Data Protection Act* in Germany.

2. Is an English translation available?

No. Only a translation of the *Federal Data Protection Act* is available. See: www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile

3. Is prior notification or approval required?

No. A notification is not required. Instead, the company data privacy protection officer ("Betrieblicher Datenschutzbeauftragter") has to be convinced of the conformity of the system.

4. Can notification or approval be filed online?

N/A

5. Generally, how long does it take to get approval?

N/A

Note that regular consultation with the Works Council is necessary and it usually takes more than three months but less than six months to conclude an agreement with the Works Council.

6. Contact information for the Data Protection Authority?

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (The Federal Commissioner for Data Protection)
Husarenstraße 30
D-53117 Bonn, Germany

T: +49 22899-7799-0
F: +49 22899-7799-550
E: poststelle@bfdi.bund.de
W: 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 on www.bfdi.bund.de.

7. What is the scope of reporting permitted?

Under the German *Federal Data Protection Act*, there are no legal restrictions regarding the scope of reporting in whistleblower programs.

However, the Düsseldorf Group and the EU 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, incorrect accounting and auditing. However, reporting is not permitted in issues concerning private or intimate life, breach of non-smoking rules, allegation of bullying.

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

No.

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

No. However, the company that establishes a procedure for whistleblower 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 Group and the EU Art. 29 working party, and as appropriate under the principle of proportionality.

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 whistleblower system.

If the employee is using the anonymous option, he/she should be asked to justify why. He/she should also be informed that misusing anonymity may prevent a whistleblower procedure from continuing. 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.

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

Yes. If the company is not Safe Harbour-certified (and has no other guarantee of an adequate level of data protection, e.g., standard contractual clauses) no data transfer outside the EU is permitted. There is no privilege for whistleblowing systems with regard to the transfer of personal data.

Data-exporting companies in Germany are not allowed to rely on the assertion of a Safe Harbour certification from U.S. companies. German data-exporting companies should demand confirmation of the certificate and compliance with the Safe Harbour principles.

Additionally, intra-group-transfer of personal data is not privileged under German law, i.e., any transfer of personal data from one legal entity to another must be justified and lawful under the *Federal Data Protection Act*. For transfers to headquarters outside the EU, this means that these must guarantee an adequate level of data protection and justify the intra-group-transfer.

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

No.

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 the Works Council.

The Works Council has joint decision-making authority with management on the introduction and operation of technical devices to monitor the behaviour or performance of the employees

and matters relating to the rules of operation of the establishment and the conduct of employees in the establishment.

Requirements for the Works Council's participation is divided into information about the implementation of a whistleblower program, negotiation and conclusion of an agreement, which usually takes six months to reach.

Prior to an agreement with the Works Council or a decision of the conciliation board, it is not possible to implement a whistleblower hotline.

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

No. Management must ensure that personal data is deleted if no longer needed. This has to be done at the latest two months after finalisation of the examination (except in cases in which personal data is necessary for further criminal proceedings or disciplinary action).

For this purpose, companies that collect personal data need to implement adequate technical measures. Such measures might be password protection, coding or logging of data input. It is within the management authority to comply with this general legal standard, particularly to prevent the use of data by unauthorized persons. The company should make sure that an internal whistleblower channel it is not run by the Human Resources department.

For more information, contact:

CMS Hasche Sigle
W: www.cms-hs.com

Carsten Domke
E: carsten.domke@cms-hs.com

GREECE

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.

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

3. Is prior notification or approval required?

Yes. According to the general provisions of the above-mentioned Act, a company must notify the DPA in writing about the establishment and operation of a file or the commencement of data processing. Assuming that in order to set a whistle blowing 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.

4. Can notification or approval be filed online?

Yes. However, it is only available in Greek.

5. Generally, how long does it take to get approval?

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

6. Contact information for Data Protection Authority?

The Hellenic Data Protection Authority
Kifissias 1-3
115 23 Athens, Greece

T: +30 210 6475600
W: www.dpa.gr

7. What is the scope of reporting permitted?

The scope of reporting is limited to accounting, internal accounting controls, auditing matters, fight against 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 though the system.

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.

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.

10. Is anonymous reporting permitted?

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

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.

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 HDPA understands that most times, 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 their fundamental freedoms are not affected.

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.

14. Are there any specific computer 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:

Bahas, Gramaridis & Partners
W: www.bahagram.com

Popi Papantoniou
E: p.papantoniou@bahagram.com

Manto Charitos
E: m.charitos@bahagram.com

INDIA

1. Applicable law and/or data protection guidelines?

At present, India does not have any specific whistleblower protection laws in place.

However, for listed companies, clause 49 of the equity listing agreement (entered into by companies for listing of their securities on a stock exchange in India) recommends adoption of a whistleblowing mechanism. It is not mandatory for a company to adopt a whistleblower policy but a company may voluntarily adopt one as a good governance practice.

Further, in relation to limited liability partnerships, Section 31 of the *Limited Liability Partnership Act, 2008* provides for a 'whistle-blower' mechanism, whereby the Tribunal has the powers to reduce or waive any penalty leviable against any partner or employee of an LLP, if it is satisfied that such partner or employee has provided useful information during an investigation of the affairs of such an LLP for finding out the offence.

Besides this, the Corporate Governance Voluntary Guidelines 2009 issued by the Government of India recommends adoption of a whistleblowing mechanism by companies.

India also has data protection legislation in place but this legislation does not directly address whistleblowers or whistleblowing programs.

2. Is an English translation available?

The equity listing agreement is available at: http://www.nseindia.com/content/equities/eq_listing.htm under the heading "Listing Agreement".

3. Is prior notification or approval required?

No.

4. Can notification or approval be filed online?

N/A

5. Generally, how long does it take to get approval?

N/A

6. Contact information for Data Protection Authority?

N/A

7. What is the scope of reporting permitted?

There is no defined scope of reporting.

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 the whistleblower policy as they deem appropriate.

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.

10. Is anonymous reporting permitted?

There is nothing specified in this regard. The companies are free to design their own policies including permitting anonymous reporting.

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

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

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 consent of the data provider.

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

No.

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:

Vaish Associates Advocates
W: www.vaishlaw.com

Bomi Daruwala
E: bomi@vaishlaw.com

Hitender Mehta
E: hitender@vaishlaw.com

IRELAND

1. Applicable law and/or data protection guidelines?

No, Ireland has no specific whistleblower protection laws in place. There is sectoral legislation which provides protection to persons making disclosures in sectors such as health care, health and safety, and immigration. The data protection guidelines are found in the *Data Protections Acts*, 1988-2003.

2. Is an English translation available?

The primary language is English. See *Data Protection Acts*: www.dataprotection.ie/documents/legal/DPAConsolMay09.pdf.

3. Is prior notification or approval required?

No.

4. Can notification or approval be filed online?

N/A

5. Generally, how long does it take to get approval?

N/A

6. Contact information for Data Protection Authority?

Office of the Data Protection Commissioner
Canal House,
Station Road,
Portarlington,
Co. Laois, Ireland

T: +353 (0)1 57 868 4800
W: www.dataprotection.ie

7. What is the scope of reporting permitted?

The scope of reporting is limited to the following fields: accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime, or if there is otherwise risk of being in breach of the DPL.

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

No.

9. Are there limits to who can be subject of a report?

No.

10. Is anonymous reporting permitted?

Yes.

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

Yes. Data transfers outside EU/EEA countries has to follow the requirements stated in the Directive 95/46/EC.

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

Yes. One of the conditions to be met for the transfer of data is that the data subject has consented to the transfer.

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

No.

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:

Mason Hayes + Curran
W: www.mhc.ie

Elizabeth Ryan
E: eryan@mhc.ie

ISRAEL

1. Applicable law and/or data protection guidelines?

No. Israel has no specific whistleblower protection laws in place.

The *Protection of Employees Law (Exposure of Offences 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").

2. Is an English translation available?

No.

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.

4. Can notification or approval be filed online?

N/A

5. Generally, how long does it take to get approval?

N/A

6. Contact information for Data Protection Authority?

The Israeli Law, Information and Technology Authority
The Government Campus, 9th floor, 125 Begin Road,
Tel Aviv, Israel
(Mailing address: P.O. Box 7360, Tel Aviv 61072, Israel)

T: +972-3-763-4050
E: ILITA@justice.gov.il
W: www.justice.gov.il/MOJEng/RashutTech/default.htm

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 filling of the complaint in good faith;

b) The complaint was submitted in relation to the commission of an offence 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;

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.

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.

9. Are there limits to 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.

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.

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 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 fulfil the conditions laid down in Israel for the maintenance and use of the information, *mutatis mutandis*;

    d) Transferring the information is essential for the defence of public welfare and security; or

    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 which has been published in the Official Gazette, that there exists in such country a designated authority to protect privacy, after it has reached at an arrangement for cooperation with such authority (to date there is no such notification).

In addition to the fulfilment of the above conditions, (with respect to both sections 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 defences that might apply. Such defences might apply in cases where the defendant or the accused committed the infringement in good faith in the following circumstances:

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 defence 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.

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.

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

Yes. 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 (if any). As a general rule, consultation with the employees' representative (if once 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.

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:

Herzog, Fox & Neeman
W: www.hfn.co.il

Nurit Dagan
E: dagan@hfn.co.il

Ilana Berman
E: bermani@hfn.co.il

ITALY

1. Applicable law and/or data protection guidelines?

No. Italy has no specific whistleblower protection laws in place.

Nonetheless, at conclusion of a series of interventions to this regard, on December 10, 2009, the Italian Data Protection Authority ("DPA") has addressed both the Italian Parliament and Government with a recommendation about the opportunity to enact adequate law provisions aimed at regulating the use of whistleblowing programs and, in general, of other systems reporting alleged violations on the side of subjects operating, under various qualifications, for a business organization (the "Recommendation").

However, no legislative or governmental initiative has followed the aforementioned Recommendation. 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 opinions on whistleblowing programs.

2. Is an English translation available?

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

3. Is prior notification or approval required?

No.

4. Can notification or approval be filed online?

N/A

5. Generally, how long does it take to get approval?

N/A

6. Contact information for Data Protection Authority?

Garante per la protezione dei dati personali
Piazza di Monte Citorio n. 121
00186 ROMA, Italy

T: +39 06.69677.1
F: +39 06.69677.785
E: garante@garanteprivacy.it
W: www.garanteprivacy.it

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, the principles and the procedures set forth by the EU Art. 29 Working Party (Opinion 1/2006) are observed by companies that want to implement a whistleblowing system. This Opinion recommends 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 (also according the Italian *Statute of Work* (L. 300/70) in issues concerning private or intimate life, breach of non-smoking rule, or allegation of bullying.

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 Art. 29 WP.

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 Art. 29 Working Party.

10. Is anonymous reporting permitted?

Yes.

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

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

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 the consent.

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

No. Nonetheless, depending on the ways by which the relevant whistleblowing program is adopted and managed, a consultation with the Work Council may be recommended.

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

No. 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 minimize, by means of suitable preventative security measures, the risk of data destruction or loss, whether by accident or not, of unauthorised 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:

Gianni, Origoni, Grippo & Partners
W: www.gop.it

Daniele Vecchi
E: dvecchi@gop.it

Melissa Marchese
E: mmarchese@gop.it

JAPAN

1. Applicable law and/or data protection guidelines?

Yes. Japan has a specific whistleblower protection law in place: *The Whistleblower Protection Act* (Law No. 122, 2004).

The protection of personal data is treated as a different issue and it is regulated by *The Act Concerning Protection of Personal Information* (Law No. 57, 2003,) which is generally referred to as the "Personal Information Protection Law". A translation of this is available at:
www.cs-trans.biz/Personal_Information.htm.

Various governmental agencies have issued data protection guidelines with respect to the businesses over which they have jurisdiction. It should be noted that the whistleblower protection is not dealt with in the Personal Information Protection Law or such industry/business-specific data protection guidelines.

2. Is an English translation available?

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

3. Is prior notification or approval required?

No.

4. Can notification or approval be filed online?

N/A

5. Generally, how long does it take to get approval?

N/A

6. Contact information for Data Protection Authority?

Consumer Affairs Agency with respect to the Personal Information Protection Law:
W: www.caa.go.jp/seikatsu/koueki/index.html

Ministry of Welfare and Labour with respect to *The Whistleblower Protection Act*:
W: www.mhlw.go.jp/otoiawase/

7. What is the scope of reporting permitted?

The whistleblowing programs generally adopted by private companies encompass the violation of laws and company morals.

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 company officers and employees can make a report.

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

Yes. Only company officers and employees may be the subject of a report.

10. Is anonymous reporting permitted?

Yes. Anonymous reporting is permitted without restriction, but investigation initiated by such anonymous reporting may be limited or not effectively conducted.

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

No. However, it should be conducted in such manner as will duly protect the personal information or other interests of others and it will also be subject to the restrictions under the Personal Information Protection Law.

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

No.

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

No.

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:

City Yuwa Partners
W: www.city-yuwa.com

Tsuneo Sato
E: tsuneo.sato@city-yuwa.com

MALAYSIA

1. Applicable law and/or data protection guidelines?

Yes. Malaysia has specific whistleblower protection laws in place.

2. Is an English translation available?

Yes. A translation is available at:
www.cljlaw.com
or
www.lawnet.com.my

(Note that both websites require registration.)

3. Is prior notification or approval required?

No.

4. Can notification or approval be filed online?

N/A

5. Generally, how long does it take to get approval?

N/A

6. Contact information for Data Protection Authority?

Not yet available. It is anticipated that a Personal Data Protection Commission will be appointed during the third or fourth quarter 2011.

7. What is the scope of reporting permitted?

Reports can be made by any person against any conduct which, if proved, constitutes a disciplinary or criminal offence. 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.

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 offence or a criminal offence.

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

No. Anyone can be a subject of a report.

10. Is anonymous reporting permitted?

Yes.

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.

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

No.

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

N/A

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

N/A

For more information, contact:

Shearn Delamore & Co.
W: www.shearndelamore.com

K Shanti Mogan
E: shanti@shearndelamore.com

THE NETHERLANDS

1. Applicable law and/or data protection guidelines?

No. The Netherlands has no specific whistleblower protection laws in place.

The only specific whistleblower legislation concerns the establishment of public bodies for the handling of abuse reports. The CIO was established by law and operates as an independent investigator of misbehaviour in the central government, police and defence sectors. The CIO has been assigned the statutory task of handling abuse reported by a whistleblower and is entitled to take protective measures and / or compensate the whistleblower.

Moreover, the Dutch government has decided it will install a referral point for whistleblowers. This referral point will be operated by a public body, the CAVK ("Commission for advice and referral point on whistleblowing"). The CAVK will be established by a specific decree, which was issued on 27 September 2011, published on October 4th and is expected to come into force late in 2011. The CAVK will not investigate reported abuse, but only advise and assist whistleblowers and refer abuses to the competent authorities. The CAVK will be assigned the task of advising and assisting whistleblowers in both the public and private sectors, and 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.

Finally, the Dutch Corporate Governance Code Monitoring Committee presented the revised Dutch Corporate Governance Code (the DCGC) on 10 December 2008. In 2004, this code was designated as a code of conduct to which listed companies should refer in their annual report, 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 are normally assessed against the statutory requirements of the Dutch *Data Protection Act* (*Wet bescherming persoonsgegevens*) and general principles of law, such as the concept of "good employership".

Several advisory bodies have rendered their opinions to the Dutch government. The DPA uses these opinions when assessing the compliance of data processing and / or transfer activities associated with whistleblower programs.

2. Is an English translation available?

No. Only the DCGC is available in English at:
www.commissiecorporategovernance.nl/page/downloads/DEC_2008_UK_Code_DEF__uk_.pdf

3. Is prior notification or approval required?

Yes.

4. Can notification or approval be filed online?

Yes.

5. Generally, how long does it take to get approval?

Less than three months when personal data is exclusively processed within the EU/EEA; three to six months in case of pan- European programs (i.e., where personal data is transferred to recipients outside the EEA).

6. Contact information for Data Protection Authority?

College Bescherming Persoonsgegevens
Postbus 93374
2509 AJ Den Hagg
Amsterdam, The Netherlands

T: +31 (0)900-2001 201
W: www.cbpweb.nl

7. What is the scope of reporting permitted?

Usually this involves any serious violations of statutory or contractual obligations depending on the nature and impact of the abuse. Financial reporting and corruption are most commonly put forward as the purpose for reporting.

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

No.

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.

10. Is anonymous reporting permitted?

Yes. However, it should be discouraged.

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

Yes.

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

No.

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*. The Works Council has a right of consent with regard to decisions on the establishment, amendment or cancellation of such procedure.

A decision to establish, amend or cancel a whistleblower program without the prior consent of the Works Council is voidable. 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.

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:

CMS Derks Star Busmann
W: www.cms-dsb.com

Wouter Seinen
E: wouter.seinen@cms-dsb.com

Silvia van Schaik
E: silvia.vanschaik@cms-dsb.com

NORWAY

1. Applicable law and/or data protection guidelines?

Yes. Norway has specific whistleblower protection laws in place.

In Norway, we have both whistleblower legislation and DPA 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 routines for internal notification or implement other measures that enable the employees to make use of the right. Such routines 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 procedure 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 applies to the processing of personal data that is reported through and collected in whistleblowing programs.

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/upload/Dokumenter/regelverk/lov_forskrift/Engelsk%20lov%20ny%20utgåve%20til%20publisering.pdf

The Personal Data Regulations:
www.datatilsynet.no/upload/Dokumenter/regelverk/lov_forskrift/Engelsk%20forskrift%20ny%20utgåve%20til%20publisering.pdf

The DPA guidelines are not available in English.

3. Is prior notification or approval required?

Yes. However, usually a license from the DPA is required because information relating to criminal offences 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.

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.

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 an orientation regarding the planned processing of personal data.

Obtaining a license takes approximately 8-10 weeks, provided that all documentation requirements are fulfilled.

6. Contact information for Data Protection Authority?

The Data Protection Authority
P.O Box 8177 Dep, N-0034
Oslo, Norway

T: +47 22 39 69 00
E: postkasse@datatilsynet.no
W: www.datatilsynet.no/

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 offences such as corruption and other types of financial crime, breaches of the company's ethic codes, hazardous working conditions 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.

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.

9. Are there limits to who can be subject of a report?

No.

10. Is anonymous reporting permitted?

Yes. Anonymous reporting is permitted and many whistleblowers prefer to stay anonymous. Usually, companies have special rules concerning this.

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:

a) The company receiving the data is Safe Harbour-certified;

b) The country is designated by the European Commission as having adequate protection;

c) The EU standard contractual clauses for transfer are used. This requires an approval from the DPA in advance;

d) 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.

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

No.

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

No. It 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.

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

Yes. The data processor 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 processor therefore has to implement both technical, physical, organizational, and personnel security measures in order to ensure satisfactory data security. The purpose is to prevent unauthorised/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 investigations unless other purposes legitimizes further storage.

For more information, contact:

Advokatfirmaet Schjødt AS
W: www.schjodt.no

Mr. Kaare Risung
E: Kaare.risung@schjodt.no

Mr. Trond Stang
E: trond.stang@schjodt.no

PORTUGAL[6]

1. Applicable law and/or data protection guidelines?

No. 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 nr 765/2009 under which it settled applicable principles to whistleblower programs.

2. Is an English translation available?

Yes. A translation is available at:
www.cnpd.pt/english/bin/legislation/Law6798EN.HTM

Resolution nr 765/2009 of the DPA is only available in Portuguese.

3. Is prior notification or approval required?

Yes. An approval from the DPA is required.

4. Can notification or approval be filed online?

Yes. The request for approval can only be filed on-line and it has to be made in the Portuguese language.

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.

6. Contact information for Data Protection Authority?

Comissão Nacional de Protecção de Dados
Rua de São Bento, 148 3º, 1200-821
Lisboa, Portugal

[6] Editors' Note: This chapter was written by former members of Cuatrecasas Gonçalves Pereira's office in Lisbon.

T: +351 213 928 400
E: geral@cnpd.pt
W: www.cnpd.pt

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.

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.

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 (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.

10. Is anonymous reporting permitted?

No.

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) The data recipient has adhered to the Safe Harbor Principles; or

c) Standard contractual clauses for the transfer of personal data are used as approved by the European Commission; or

d) 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).

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 defence of legal claims. When transfer is made to a data processor in a country than ensures an adequate level of protection, the DPA authorizes the transfer (e.g., subscription of Safe Harbour Principles, Standard clauses as approved by the European Commission).

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.

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

Yes. Resolution nr 765/2009 of the DPA indicates the following as the minimum acceptable for data security:

a) The computerised system should be organised in a way as to allow data access only upon user's identification and individual password or any other authentication mechanism, to be renewed from time to time;

b) All data accesses should be recorded and regularly monitored;

c) Access to servers should be restricted to authorised personnel only (physical and computerised access);

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;

c) In cases where disciplinary or judicial procedures take place, data shall be kept until these procedures are finished.

For more information, contact:

PLMJ
W: www.plmj.pt

Daniel Reis
E: daniel.reis@plmj.pt

Marta Costa
E: marta.costa@plmj.pt

SOUTH AFRICA

1. Applicable law and/or data protection guidelines?

Yes. South Africa has specific whistleblower protection laws in place. The *Protected Disclosures Act 26 of 2000* ("the PDA") applies to any disclosure of information regarding any conduct of an employer or another employee, which is made by any employee who has reason to believe that the relevant information shows that an offence has been, is being or will be committed.

South Africa does not have comprehensive data protection legislation in place but there is an ongoing drafting process.

2. Is an English translation available?

Yes. A translation is available at:
www.dac.gov.za/acts/Protected%20Disclosures%20Act.pdf

3. Is prior notification or approval required?

No.

4. Can notification or approval be filed online?

N/A

5. Generally, how long does it take to get approval?

N/A

6. Contact information for Data Protection Authority?

N/A

7. What is the scope of reporting permitted?

The PDA applies to any disclosure of information regarding any conduct of an employer or another employee, which is made by any employee who has reason to believe that the relevant information shows that an offence has been, is being or will be committed.

The reporting is accordingly not limited to financial matters only but also includes disclosures relating to any criminal conduct, health or safety, the environment and unfair discrimination.

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 may make a protected disclosure.

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

The PDA provides for disclosures of information relating to any employer (including any company official) or to any other employee.

10. Is anonymous reporting permitted?

Yes. The DPA does not specifically prevent anonymous whistleblowing. However, the purpose of the South African whistleblowing legislation is in fact to prevent victimisation, recrimination or dismissal of employees who make disclosures, so most disclosures will not be anonymous.

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

No.

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

No.

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

No.

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:

Webber Wentzel
W: www.webberwentzel.com

Dario Milo,
E: dario.milo@webberwentzel.com

SPAIN

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"; see: www.privacyconference2009.org/media/Publicaciones/common/guia_relaciones_labourales.pdf 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).

2. Is an English translation available?

No.

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 Director of the DPA.

4. Can notification or approval be filed online?

N/A

5. Generally, how long does it take to get approval?

N/A

6. Contact information for Data Protection Authority?

Spanish Data Protection Authority (Agencia Española de Protección de Datos)
C/ Jorge Juan, 6
28001 - Madrid (Spain).

T: +34 901 100 099 or +34 912 663 517
W: www.agpd.es

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.

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.

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

No. As a general principle, the companies are free to design their programs as they deem appropriate, without applying any specific regulatory restriction in this respect.

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.

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 summarised below:

a) 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.

b) International transfers: If the entity to which the personal data is going to be communicated is 1) established in the EU, 2) is Safe Harbour-certified or 3) 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:
   i. the affected individuals are informed in advance about the identity of the third party gaining access to their personal data and, when applicable, consent to such access; and
   ii. a notification of the international transfer is filed before the DPA.

If the addressee of the personal data is not included in one of the three categories mentioned in b) above, the international transfer may be done as long as the following requirements are met:

i. the affected individuals are informed in advance about the identity of the third party gaining access to their personal data and, when applicable, consent such access; and
ii. express and prior authorisation is given by the director of the DPA.

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 11 above.

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

Yes. 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 programs falls within the scope of this obligation, requiring the company to inform said council on the main features of the program to be launched.

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, there are no specific regulations dealing with the whistleblower program (in particular, with respect to deletion, according to the law, the personal data must be cancelled when they are no longer necessary or appropriate for the purpose for which they were collected or registered).

For more information, contact:

Cuatrecasas, Gonçalves Pereira, S.L.P.
W: www.cuatrecasas.com

Jorge Llevat
E: jorge.llevat@cuatrecasas.com

Jorge Monclús
E: jorge.monclus@cuatrecasas.com

SWEDEN

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 new 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.:

a) 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.

b) 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.

c) Only key personnel and employees in a management position may be reported and only they may be processed in the system.

d) 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.

2. Is an English translation available?

Yes. A translation is available at:
www.datainspektionen.se/in-english/legislation/the-personal-data-act/

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 1 above.

An exemption would be required if the company wishes to deviate from the requirements set out in the answer to Question 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 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.

4. Can notification or approval be filed online?

No.

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 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.

6. Contact information for Data Protection Authority?

Datainspektionen
Box 8114
104 20 Stockholm, Sweden

T: +46 08 657 61 00
E: datainspektionen@datainspektionen.se
W: www.datainspektionen.se/

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.

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.

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 reported and only such employees may be processed in the system.

10. Is anonymous reporting permitted?

Yes.

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.

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, Safe Harbour-certification, the Model Clauses or any other adequate security level.

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.

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:

Setterwalls Advokatbyrå AB
W: www.setterwalls.se

Fredrik Roos
E: fredrik.roos@setterwalls.se

Bobi Mitrovic
E: bobi.mitrovic@setterwalls.se

SWITZERLAND

1. Applicable law and/or data protection guidelines?

No. Switzerland has no specific whistleblower protection laws in place.

Various guidelines exist, but all of them on a private level.

2. Is an English translation available?

N/A

3. Is prior notification or approval required?

N/A

4. Can notification or approval be filed online?

N/A

5. Generally, how long does it take to get approval?

N/A

6. Contact information for Data Protection Authority?

Eidgenoessischer Datenschutz und Oeffentlichkeitsbeauftragter
Feldeggweg 1
3005 Bern, Switzerland

T: +41 31 322 43 95
W: www.edoeb.admin.ch

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.

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 they are going to accept.

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

No.

10. Is anonymous reporting permitted?

Yes.

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.

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. The same is true for a transfer to the US *provided that* the U.S. entity has subscribed to Safe Harbour.

If neither of the above apply, consent may be required, depending on whether the reported conduct is a criminal offence (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).

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

N/A

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:

CMS von Erlach Henrici AG, Zurich
W: www.cms-veh.com

Dr. Robert G. Briner,
E: robert.briner@cms-veh.com

THAILAND

1. Applicable law and/or data protection guidelines?

Thailand has no specific whistleblower protection laws in place.

Some principles and guidelines can be found in the Constitution of Thailand.

Thailand has been a full participant of the *Organization for Economic Co-operation and Development* (OECD) Development Centre 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. The latest review of the draft took place in 2008. However, there is no reference made to whistleblower programs in the bill.

2. Is an English translation available?

N/A

3. Is prior notification or approval required?

N/A

4. Can notification or approval be filed online?

N/A

5. Generally, how long does it take to get approval?

N/A

6. Contact information for Data Protection Authority?

N/A

7. What is the scope of reporting permitted?

N/A

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

N/A

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

N/A

10. Is anonymous reporting permitted?

N/A

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

N/A

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

N/A

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

N/A

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

No. The only requirement is that the system administer of a network maintain computer traffic records for a minimum of 90 days in order meet statutory requirements regarding official requests for backtracking investigations as required by the *Computer Crime Act A.D. 2007*.

For more information, contact:

Chandler & Thong-EK Law Offices
W: www.ctlo.com

Niwes Phancharoenworakul
E: niwes@ctlo.com

Chadaporn Ruangtoowagoon
E: chadaporn@ctlo.com

TURKEY

1. Applicable law and/or data protection guidelines?

No. Turkey has no specific whistleblower protection laws in place.

There is no legislation that directly governs collection, processing, transfer and/or protection of personal data. Even though Turkey has signed the Council of Europe's Convention for the Protection of Individuals (the "Convention") with regard to Automatic Processing of Personal Data in the year 1981, the Convention has not been implemented.

As the primary basis for the protection of data, Paragraph 3 of Article 20 of the Turkish *Constitution* provides that:

"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 full consent of the concerned person. Principles and procedures regarding the protection of personal data shall be prescribed by law."

A draft Law for the Protection of Personal Data (the "Draft Bill") has been prepared to meet Turkey's obligations under the Convention, but it has long been pending and under discussion for enactment.

In the absence of directly applicable legislation on data collection, processing or transfer, the legal framework applicable to data protection is determined by way of interpretation of the general principles of the *Constitution*, *the Civil Code*, the *Code of Obligations*, the *Commercial Code*, the *Criminal Code* and other applicable secondary legislations.

2. Is an English translation available?

N/A

3. Is prior notification or approval required?

N/A

4. Can notification or approval be filed online?

N/A

5. Generally, how long does it take to get approval?

N/A

6. Contact information for Data Protection Authority?

N/A

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.

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

No. Only an age limitation on the question of reporting may exist.

9. Are there limits to who can be subject of a report?

No.

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.

11. Are there restrictions to the transfer of data in a whistleblowing program?

Yes. The employee's consent is required for the transfer of data. We recommend obtaining a written consent from the employees in advance before any transfer and sharing of personal data with third parties.

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

No. However, obtaining consent is recommended.

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.

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

No, provided that the relevant personal data is deleted promptly.

For more information, contact:

Hergüner Bilgen Özeke Attorney Partnership
W: www.herguner.av.tr

Mr. Kemal Mamak
E: kmamak@herguner.av.tr

Ms. Bige Göksel
E: bgoksel@herguner.av.tr

UNITED KINGDOM

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 victimisation and/or dismissal. A protected disclosure is a disclosure that a worker makes in good faith, reasonably believing that the information tends to show malpractice within the company. 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. 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".

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.

U.K. Employment Tribunals have the power to send details of an individual's whistleblowing claim to a prescribed regulator if the claimant gives his/her express consent (simply by ticking a box on the claim form). There are a large number of prescribed regulators, which includes the U.K. Information Commissioner (our data protection watchdog). The regulator will then have the opportunity to decide whether the issue highlighted in the claim form requires investigation.

The government has indicated that it will be introducing new protections for public sector whistleblowers although no details on these are available at time of writing.

2. Is an English translation available?

The primary language is English.

The Employment Rights Act 1996:
www.opsi.gov.uk/acts/acts1998/ukpga_19980023_en_1

3. Is prior notification or approval required?

No.

4. Can notification or approval be filed online?

N/A

5. Generally, how long does it take to get approval?

N/A

6. Contact information for Data Protection Authority?

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow, Cheshire, United Kingdom SK9 5AF

T: + 44 0303 123 1113
W: www.ico.gov.uk

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:

- criminal offences;
- breach of any legal obligation;
- miscarriages 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.

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.

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 8 above.

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.

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 DPL 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. There are, however, some relaxations of the legislation, for example for transfers within the EU and for transfers to the U.S. where the transfer is made to companies which are Safe Harbour-certified.

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, DPL 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 DPL (which includes information about the commission or alleged commission of an offence). 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.

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

No.

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 requires 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 DPL.

For more information, contact:

McClure Naismith LLP
W: mcclurenaismith.com

David Gourlay
E: dgourlay@mcclurenaismith.com

Wragge & Co LLP
W: wragge.com

Jonathan Chamberlain
E: jonathan_chamberlain@wragge.com

UNITED STATES OF AMERICA

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 against 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, applies to employees of publicly traded companies, as noted above.

***Dodd–Frank Wall Street Reform and Consumer Protection Act* (Pub.L. 111-203, H.R. 4173).** The Act, known as the *Dodd-Frank Act*, is a federal statute – signed into law on July 21, 2010 – which significantly increased 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 Securities and Exchange Commission ("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.

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 on the internet at the following locations:

False Claims Act: http://www.taf.org/federalfca.htm

Sarbanes-Oxley Act: http://uscode.house.gov/download/pls/15C98.txt

SEC Regulations: http://www.sec.gov/rules/final/33-8220.htm

Dodd-Frank Act: http://www.sec.gov/about/laws/wallstreetreform-cpa.pdf

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. The United States does not have a Data Protection Authority per se, but agencies like the Federal Trade Commission (FTC), and state Attorneys General do have oversight and enforcement authority in particular discrete areas, including privacy.

4. Can notification or approval be filed online?

N/A

5. Generally, how long does it take to get approval?

N/A

6. Contact information for Data Protection Authority?

N/A

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 subject matter limits in particular laws, as discussed in No. 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.

8. Are there limits on 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).

9. Are there limits as to who can be 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 Q. 7 and 8.

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.

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 and EU country data 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).

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.

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 behaviour), 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.

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:

Edwards Wildman Palmer LLP
www.edwardswildman.com

Mark E. Schreiber
E: mschreiber@edwardswildman.com

David C. Kurtz
E: dkurtz@edwardswildman.com

WLG MEMBER FIRMS PRIVACY & DATA PROTECTION CONTACTS

ARGENTINA

Alfaro-Abogados
Ms. Soledad Matteozzi
T: +1 212 698 1147
E: smatteozzi@alfarolaw.com

Mr. Pedro Mazer
T: +54 11 4393 3003

AUSTRALIA

Minter Ellison
Mr. Charles Alexander
T: +61 2 9921 4826
E: charles.alexander@minterellison.com

AUSTRIA

CMS Reich-Rohrwig Hainz Rechtsanwälte GmbH
Mr. Bernt Elsner
T: +43 1 40443 1850
E: bernt.elsner@cms-rrh.com

Mr. Robert Keisler
T: +43 1 40443 2850
E: robert.keisler@cms-rrh.com

BELGIUM

CMS DeBacker
Mr. Veerle Raus
T: +32 2 743 69 74
E: veerle.raus@cms-db.com

CANADA

Davies Ward Phillips & Vineberg LLP
Mr. Stéphane Eljarrat
T: +1 514 841 6439
E: seljarrat@dwpv.com

Goodmans LLP
Mr. Peter Ruby
T: +1 416 597 4184
E: pruby@goodmans.ca

CHILE

Urenda, Rencoret, Orrego y Dörr
Mr. Ignacio Barón
T: +56 (2) 499 5540
E: ibaron@urod.cl

Mr. Nicholas Mocarquer
T: +56 (2) 499 5531
E: nmocarquer@urod.cl

CZECH REPUBLIC

Havel, Holásek & Partners s.r.o.
Mr. Robert Nešpůrek
T: +420 224 895 950
E: robert.nespurek@havelholasek.cz

Richard Otevřel
T: +420 224 895 943
E: richard.otevrel@havelholasek.cz

DENMARK

Beck-Bruun
Arly Carlquist,
T: +45 72 27 34 62
E: ac@bechbruun.com

Ms. Birgitte Toxværd
T: +45 72 27 33 84
E: bit@bechbruun.com

FINLAND

Castrén & Snellman Attorneys Ltd.
Ms. Eija Warma
T: +358 (0) 20 7765 376
E: eija.warma@castren.fi

FRANCE

Soulier Avocats
Ms. Emilie Ducorps-Prouvost
T: +33 (0) 1 40 54 29 29
E: e.ducorpsprouvost@soulier-avocats.com

Ms. Laure Marolleau
T: +33 (0) 1 40 54 29 29
E: l.marolleau@soulier-avocats.com

GERMANY

CMS Hasche Sigle
Mr. Christian Runte
T: +49 89 23807 163
E: christian.runte@cms-hs.com

Mr. Carsten Domke
T: +49 221 7716 305
E: carsten.domke@cms-hs.com

GREECE

Bahas, Gramaridis & Partners
Mr. Popi Papantoniou
T: +(30) 210 3318170
E: p.papantoniou@bahagram.com

Mr. Manto Charitos
T: +(30) 210 3318170
E: m.charitos@bahagram.com

INDIA

Vaish Associates Advocates
Mr. Bomi Daruwala
T: +91 22 4213 4123
E: bomi@vaishlaw.com

Mr. Hitender Mehta
T: +91 124 454 1001
E: hitender@vaishlaw.com

IRELAND

Mason Hayes + Curran
Ms. Elizabeth Ryan
T: +353 1 614 50001
E: eryan@mhc.ie

ISRAEL

Herzog, Fox & Neeman
Mr. Nurit Dagan
T: +972 3 692 7424
E: dagan@hfn.co.il

Ms. Ilana Berman
T: +972 3 692 2045
E: bermani@hfn.co.il

ITALY

Gianni, Origoni, Grippo & Partners
Mr. Daniele Vecchi
T: +39 02 763741
E: dvecchi@gop.it

Ms. Melissa Marchese
T: +39 02 763741
E: mmarchese@gop.it

JAPAN

City Yuwa Partners
Mr. Tsuneo Sato
T: +81 3 6212 5500
E: Tsuneo.sato@city-yuwa.com

MAYLASIA

Shearn Delamore & Co.
Mr. K Shanti Mogan
T: +603 2027 2921
E: shanti@shearndelamore.com

THE NETHERLANDS

CMS Derks Star Busmann
Mr. Wouter Seinen
T: +31 30 2121 191
E: wouter.seinen@cms-dsb.com

Ms. Silvia van Schaik
T: +31 30 2121 640
E: silvia.vanschaik@cms-dsb.com

NORWAY

Advokatfirmaet Schjødt AS
Mr Kaare Risung
T: +47 23 01 18 33
E: kmr@schjodt.no
Mr. Trond Stang
T: +47 22 01 88 00
E: trond.stang@schjodt.no.

PORTUGAL

PLMJ
Daniel Reis
T: + 351 21 319 73 00
E: daniel.reis@plmj.pt

Luís Sobral
T: + 351 21 319 73 00
E: luis.sobral@plmj.pt

SOUTH AFRICA

Webber Wentzel
Mr. Dario Milo
T: +27 11 530 5232
E: dario.milo@webberwentzel.com

SPAIN

Cuatrecasas, Gonçalves Pereira, S.L.P.
W: www.cuatrecasas.com
Mr. Jorge Llevat
T: +34 93 312 7196
E: jorge.llevat@cuatrecasas.com

Mr. Jorge Monclús
T: +34 932 905 500
E: jorge.monclus@cuatrecasas.com

SWEDEN

Setterwalls Advokatbyrå AB
Mr. Fredrik Roos
T: +46 31 701 17 00
E: fredrik.roos@setterwalls.se

Ms. Bobi Mitrovic
T: +46 31 701 17 55
E: bobi.mitrovic@setterwalls.se

SWITZERLAND

CMS von Erlach Henrici AG, Zurich
Dr. Robert G. Briner
T: +41 44 285 11 11
E: robert.briner@cms-veh.com

THAILAND

Chandler & Thong-EK Law Offices
Mr. Niwes Phancharoenworakul
T: +66 2 266 6485
E: niwes@ctlo.com

Ms. Chadaporn Ruangtoowagoon
T: +66 2 266 6485
E: chadaporn@ctlo.com

TURKEY

Hergüner Bilgen Özeke Attorney Partnership
Mr. Kemal Mamak
T: +90 212 310 1812
E: kmamak@herguner.av.tr

Ms. Bige Göksel
T: + 90 212 310 1800
E: bgoksel@herguner.av.tr

UNITED KINGDOM

McClure Naismith LLP
Mr. David Gourlay
T: +44 (0) 131 272 8377
E: dgourlay@mcclurenaismith.com

Wragge & Co LLP
Mr. Jonathan Chamberlain
T: +44 (0) 141 204 2700
E: jonathan_chamberlain@wragge.com

UNITED STATES

Edwards Wildman Palmer LLP
Mr. Mark Schreiber
T: +1 617 239 0585
E: mschreiber@edwardswildman.com

David C. Kurtz
T: +1 617 239 0213
E: dkurtz@edwardswildman.com