THE Network
Integrated GRC Solutions

White Paper

Best Practices Guide for Global Ethics Hotlines

A Guide To Navigating Hotline Compliance Guidelines Worldwide

Table of Contents

An Overview of Global Ethics Best Practices

Established first in the U.S. as a tool to help identify corporate crime, hotline/whistleblower programs have expanded to cover nearly every aspect of business practice and provide employees with a channel to report all kinds of misconduct or malfeasance.

In today's global marketplace, companies are continuing to expand beyond their borders and into neighboring and distant countries. Whether the goal is to attract new consumers, outsource jobs or create new business channels, the importance in establishing a symbiotic relationship between your organization and a country's unique cultural and legal structure is crucial to your success.

Let's start by taking a general view of corporate governance rules and how they guide a corporation's actions and endeavors. Corporate governance serves as an umbrella to protect shareholders, employees and citizens, impacting how corporations execute internal and external accounting controls, the establishment of an independent board, the reporting, transfer and storage of data, and more. In the wake of corporate scandals, governments worldwide have enacted corporate governance regulations to restore public trust in corporations by enhancing transparency and accountability. An important element of these regulations is the encouragement of channels to report corporate misconduct without fear of retaliation.

As a multi-national corporation, it is critical when beginning to do business in any country that you have a thorough understanding of the laws and culture of that country, and how they might affect the establishment of an effective hotline. In the United States, the Federal Sentencing Guidelines for Organizations (FSGO), the Sarbanes-Oxley Act (SOX) and the Dodd-Frank Act have strongly supported the case for an expansive employee complaint process emphasizing the possibility of anonymous hotline reporting.

Although only mandated for publicly-traded companies, hotlines have been widely employed by private corporations, governments, colleges & universities and non-profits as part of their business strategy to promote organizational health. As these organizations expand to different countries, they must be sensitive to differing approaches to corporate governance and employee relations which may challenge the assumptions underlying existing whistleblower complaint processes.

In Europe, for example, distrust of whistleblowers has historical roots. During World War II, those who sought favors from the Nazi occupiers by informing on others were reviled by their countrymen. Thus, France in particular has issued strict guidelines for hotline operation reflecting a distaste for whistleblowers, especially anonymous ones. It is important when venturing into different cultures not only to follow the country's specific legal guidelines for hotline operation, but also to respect cultural differences in order to create an effective communication and awareness campaign to promote the program.

Keeping up with regulations relating to corporate hotlines and whistleblowing programs demands increased scrutiny at every layer of the company, from legal to operations to communications to human resources. The information found in this reference guide is meant to serve as a starting point for hotline compliance in the global marketplace.

When establishing a program to effectively span the globe, there are several key areas where hotline regulations differ among countries. They are:

- Caller Anonymity
- Scope of Hotline
- Data Protection, Transfer and Retention
- Whistleblower Retaliation
- Reporting Parameters

GLOBAL ETHICS BY REGION:

North America

United States of America

Enacted in 2002, the Corporate and Criminal Fraud Accountability Act (Sarbanes-Oxley, or SOX) served as the catalyst for many other countries in enacting corporate reform, including hotlines, anonymous reporting and whistleblower protection.

SOX mandates that the Boards of publicly-held U.S. companies implement an anonymous employee complaint process not only in a company's domestic operations but worldwide. The effort to comply with that legislation outside of the U.S. has provoked differing opinions and resulted in hotline regulation in other countries, especially the European Union.

Remember that the Enron financial and accounting scandal which led directly to the enactment of SOX was revealed by an internal whistleblower. In addition to its requirement that the audit committee of the board establish a process for collecting anonymous reports of financial misconduct, SOX also includes stringent anti-retaliation provisions aimed at protecting whistleblowers.

Although SOX is focused on financial and accounting issues, U.S. hotlines are not limited in scope and allow for the reporting of additional topics such as sexual harassment and other forms of misconduct.

Summary: Corporate and Criminal Fraud Accountability Act of 2002 (Sarbanes-Oxley Act):

1. Covers publicly-held companies
2. Anonymous reporting opportunity is required
3. Protects whistleblowers from retaliation
4. Broad acceptance of different types of reports, although focus is on financial and accounting matters

The SOX whistleblower requirements made mandatory what was already strongly recommended in the FSGO. First issued in November 1991 to address individual executive responsibility for corporate crime, the FSGO was amended in 2004 in the wake of SOX. The revised FSGO makes clear that a hotline should include the possibility of anonymous reporting, and confirm that the scope should not be restricted to accounting issues.

The FSGO was established to motivate organizations to police themselves to ensure legal compliance. It prescribes seven steps that should be followed to establish an effective corporate compliance program. The step that focuses on hotlines encourages corporations to establish monitoring, auditing and reporting systems by creating and publicizing a system whereby employees and other agents can report criminal conduct without fear of retribution.

The FSGO applies to almost all types of organizations including private and public corporations, partnerships, unions, not-for-profit organizations and trusts. The premise is that the organization's executives are responsible for wrongful acts when acting in their official capacity. An organization that establishes and enforces a corporate compliance program following the prescribed seven steps may lessen or eliminate penalties levied against its executives if misconduct is subsequently uncovered, provided the executives were not involved or had no knowledge of the illegal activity.

Summary: Federal Sentencing Guidelines for Organizations - United States Sentencing Commission. Published in 1991, Amended in 2004:

1. Impacts all U.S. organizations
2. Seven recommended steps for an effective compliance program
3. Essential step is the establishment of an employee complaint process
4. Holds company liable for acts committed by employees, but relieves innocent executives from penalties if an effective compliance program is in place

Resources for the United States of America

www.ethics.org/resource/federal-sentencing-guidelines
www.ussc.gov/Guidelines/index.cfm

Canada

Quickly following the passage of SOX in the U.S., in 2003 the Canadian Security Commission Administrators (SCA) proposed a series of Multilateral Instruments to the Canadian Provinces. This included Multilateral Instrument 52-110, which required that an independent Audit Committee of the Board have oversight of a variety of accounting controls, including the receipt, retention and treatment of complaints received regarding accounting, internal accounting controls, or auditing matters. The complaint process must allow for the confidential, anonymous submission by employees, customers or third parties of their accounting or auditing concerns. This language mirrors the hotline provision in SOX. Multilateral Instrument 52-110 has been adopted in all Canadian provinces except British Columbia.

To protect public employee whistleblowers from retaliation, the Public Servants Disclosure Protection Act (Bill C-11) was passed in October 2005.

Summary: Canadian Security Commission Administrators (SCA) Multilateral Instrument 52-110 2004:

1. Impacts public companies
2. Same hotline requirement as SOX
3. Anonymous reporting opportunity is required
4. In effect in all provinces except British Columbia

Resources for Canada

www.gov.ns.ca/nssc/docs/mi52-110.pdf

GLOBAL ETHICS BY REGION:

Europe

European Union

In its Charter, the European Union established a right to personal data privacy and enunciated nine data privacy principles (Article 29). The EU directed each member country to enact data privacy legislation and establish a governmental agency for its enforcement. The EU model of data privacy is much more protective than in the U.S. Following the enactment of Sarbanes-Oxley in the United States, two high-profile cases in EU member countries (Wal-Mart/Germany, McDonald's/France) refused to allow U.S. based companies to implement complaint processes necessary for compliance with SOX.

After the McDonald's case, the French data privacy agency, CNIL (see "France" on page 10), issued stringent guidelines for hotlines in France. The EU Article 29 Working Party then issued an opinion on hotline/whistleblower programs echoing the CNIL's guidelines. Although not binding on EU member states, the Working Party's opinion is very persuasive to European data privacy agencies looking at this issue.

The Working Party opinion advocates:

- Restricting scope of hotline to finance and accounting, and to those employees involved in these matters
- Local handling of complaints
- Short-term data destruction
- Discouragement of anonymous reporting

The restrictions recommended by the Working Party opinion seemed to undermine the intent of SOX Section 301 to create a tool for employees to speak up without fear of retaliation about misconduct in the workplace. An exchange of correspondence between the EU Working Party and the U.S. Securities and Exchange Commission went a long way in reconciling the European point of view with Sarbanes-Oxley compliance. On all but the last point – anonymity – the Working Party agreed that its opinion could be interpreted flexibly to allow the Audit Committees of U.S. companies operating in Europe to establish and maintain employee hotlines in compliance with SOX.

A separate issue that poses a challenge for U.S. companies operating hotlines in Europe is the EU's strict rules on the transfer of electronic data from the EU to other countries that do not have the same high standards of personal data protection. The EU's position

on data transfer was not crafted with regard to the kind of personal data transferred in hotline calls. However, compliance with one or more of the three methods authorized by the EU is essential to establish a hotline service using a U.S. based provider. They are:

1. Safe Harbor Certification of the data recipient outside the EU (the data importer)
2. Inclusion of Standard Contract Clauses in the agreement between the data exporter and data importer
3. The data importer's adoption and enforcement globally of a privacy policy that reflects the EU's data privacy principles

The Network, as a data importer, has obtained and maintains Safe Harbor certification from the U.S. government, thus committing to uphold the EU's data privacy principles with regard to all transfers from the EU to The Network, including the initial hotline report. We also suggest the attachment of the EU standard contract clauses to our client agreements to protect downstream transfer from The Network to the U.S. offices of our clients. Adopting and enforcing a worldwide privacy policy in compliance with EU principles is a further way to demonstrate compliance.

United Kingdom

The United Kingdom's attitude to whistleblowers follows more closely that of North America, rather than mainland Europe. In 1999, prior to SOX and similar legislation developed in response to corporate malfeasance, the United Kingdom had put in place the Public Interest Disclosure Act (PIDA). This Act's main focus was to protect whistleblowers in specific situations so that employees could raise concerns outside the company without fear of retribution.

Summary: Public Interest Disclosure Act (PIDA), 1999:

1. Protects whistleblowers
2. Defined situations for employees to raise concerns outside the company
3. Voids employment contracts when applicable

In response to financial scandals in the U.S. and elsewhere, the U.K. Combined Code for Corporate Governance was revised in 2003 to state that audit committees should review arrangements by which employees may (in confidence) raise concerns about possible improprieties. An objective of the audit committee should be to ensure that arrangements are in place for the proportionate and independent investigation of such matters and for appropriate follow-up.

However, the United Kingdom, as an EU member, has established a data privacy protection agency, and although no formal guidelines on hotlines have been issued, the United Kingdom generally follows the EU in regard to data privacy principles as well as the storage and transfer of data.

France

France is recognized by most experts in the hotline compliance industry as the country within the European Union that has led the way in establishing stringent policies in regard to reporting, data storage and protection of those named in a whistleblower report. The Commission Nationale de l'Informatique et des Libertes (CNIL), issued guidelines in November 2005 on the scope of hotlines, and how data should be collected, stored, and transferred. For example, reports should only relate to financial and accounting topics, collected data should be destroyed within two months after a complaint has been investigated and a decision or ruling has been made, and anonymous reporting is strongly discouraged. A key emphasis in the CNIL's guidelines that is reflected in other European countries' guidelines is that the hotline should serve merely as a supplement to traditional internal reporting processes.

In December 2009, a French court ruled that hotlines should be strictly restricted in scope to financial and accounting issues, with no exceptions. In late 2010, the CNIL revised its guidance to reflect this ruling and eliminated the exception to the restricted scope of the hotline for issues of vital interest to the organization.

Summary: Commission Nationale de l'Informatique et des Libertes, 2005 (per revised guidance, 2010):

1. Anonymous reporting is not encouraged, only allowed in extreme circumstances
2. Data should be destroyed within two months of conclusion of investigation or other proceedings
3. Reports should relate to financial and accounting topics
4. Local handling of complaints by a dedicated unit is required to preserve confidentiality
5. Unsubstantiated data must be deleted immediately
6. The person accused of wrongdoing should be promptly notified
7. Hotlines should serve as a supplement to normal internal reporting processes

To establish a hotline in France, all companies must apply to the CNIL for authorization. The CNIL has established a simple authorization process for those hotlines that certify compliance with CNIL guidelines. In effect, certification of compliance ensures immediate approval. Those companies who are unwilling to certify compliance will have their applications scrutinized, and any departure from the guidelines will need to be justified.

Based on the sweeping nature of the CNIL's guidelines, hotline experts will typically guide corporations entering the European Union to use them as their standard for a hotline anywhere in the EU, as adherence to the French rules will typically ensure compliance with guidelines set by other EU states.

Resources for France

www.cnil.fr/english/
www.cnil.fr/dossiers/travail/actualites/article/alertes-professionnelles-la-cnil-clarifie-son-autorisation-unique-nau-004/
https://www.correspondants.cnil.fr/CilExtranetWebApp/declaration/declarant.action
http://www.herbertsmith.com/NR/rdonlyres/C9A81A2E-ED96-4F95-975B-B23B6E7D7AEE/18624/HSPO_CNIL_022011_Eng_AN_OM_SENT.html#page=1

Spain

The Spanish Data Protection Agency – Agencia Espanola de Proteccion de Datos (AEPD) – has not issued guidelines for the implementation of a whistleblower scheme/hotline. However, it has issued an opinion as a response to an application from a Japanese pharmaceutical company that provides a basis for predicting future rulings. This opinion generally follows the CNIL guidance and the EU Article 29 Working Party opinion in terms of data storage, processing, transfer and protection but has a broader acceptance of reporting topics outside the scope of financial and accounting matters.

However, the AEPD departs from the CNIL and the Working Party opinion in prohibiting, rather than discouraging, anonymous reports. The AEPD opinion states that having procedures that guarantee the confidential handling of reports, so that the accused person cannot identify his/her accuser, eliminates the need to accept an anonymous report under any circumstances.

Summary: Agencia Espanola de Proteccion de Datos (AEPD) Opinion 1/2006:

1. Generally follows CNIL and EU Article 29 Working Party
2. Provides for broader acceptance of reporting topics (outside of finance and accounting)
3. Does not accept anonymous reports
4. States data transfer should follow EU-approved standard clauses
5. Requires data to be deleted when it ceases to be necessary

Germany

In February 2005, Wal-Mart encountered opposition in Germany to the implementation of a hotline as part of its ethics program, not because of any data privacy issues, but because it did not consult its works council (German equivalent of the labor union) before announcing the implementation. This case served as a precursor for Germany's guidance on whistleblower hotlines. However, compliance with the guidelines does not obviate the requirement of negotiation with the works council.

Issued in April 2007, the German Ad-Hoc Working Group's opinion as it relates to employee data protection generally follows the guidelines set by the EU Working Party. The German opinion discourages anonymous reporting in all but exceptional cases, and all whistleblowing schemes must serve as a supplement to traditional reporting channels. It also follows the established protocol for data storage, collection, transfer and protection. One area in which the German opinion does expand upon the Working Party's guidelines is in its scope of reporting topics, as it allows for reporting beyond purely financial or accounting topics. The guidelines recommend consultation with local data protection authorities in the event of uncertainty. Notification is required if the company has no data privacy officer.

Summary: German Ad-Hoc Working Group Opinion on Employee Data Protection, April 2007:

1. Generally follows EU Working Party
2. Discourages anonymity – only in exceptional cases
3. Whistleblowing procedures should serve only as an additional reporting mechanism
4. Scope of hotline may include ethics issues beyond financial and accounting issues

Resources for Germany

www.upf.edu/iuslabor/032005/art11.htm
www.complianceweek.com/s/documents/german_whistling.pdf

Belgium

In November 2006, the Belgian Data Protection Authority (DPA) issued a recommendation regarding the compatibility of hotline programs with the Belgian Data Protection law. The recommendation generally follows EU and CNIL guidelines but expands the permitted scope beyond financial and accounting topics. The guidance sets out basic principles with regard to admissibility, scope, proportionality, accuracy, transparency, security, rights of the persons involved, and registration of the database with the Belgian DPA. The DPA should be notified about hotline implementation.

Summary: Belgian Data Privacy Commission Recommendation No. 1/2006:

1. Generally similar to EU and CNIL guidelines
2. Encourages confidentiality but will accept anonymous reports
3. Provides a broader scope of topics for reporting (beyond financial and accounting)
4. Whistleblowing system must be supplemental to internal reporting channels
5. Data transfers to a country outside the EU for only critical issues that mandate escalation
6. Data privacy rules apply for data transfers
7. Data is stored only until no longer necessary for the investigation

Resources for Belgium

www.privacycommission.be/fr/docs/Commission/2006/recommandation_01_2006.pdf

The Netherlands

The Code of Corporate Governance in the Netherlands was revised in 2003 to require businesses to establish an employee complaint process:

> "The management board shall ensure that employees have the possibility of reporting alleged irregularities of a general, operational and financial nature in the company to the chairman of the management board or to an official designated by him, without jeopardizing their legal position. Alleged irregularities concerning the functioning of management board members shall be reported to the chairman of the supervisory board. The arrangements for whistleblowers shall in any event be posted on the company's website."

The Dutch Data Protection Authority (Dutch DPA), similar to its Belgian neighbors, prefers a system that promotes confidentiality over anonymous reporting, in the belief that anonymity may foster false reports and that reports not made anonymously are easier to investigate.

Summary: Dutch Data Privacy Authority

1. Generally similar to EU and CNIL guidelines
2. Encourages confidentiality but will accept anonymous reports
3. Whistleblowing system must be supplemental to internal reporting channels
4. Data transfers to a country outside the EU for only critical issues that relate to accounting or auditing matters
5. Scope may go beyond finance and accounting
6. Data is stored no longer than two months after the conclusion of an investigation

Ireland

The Irish Data Protection Commissioner has posted guidance on hotlines and Sarbanes-Oxley compliance which generally follow the Working Party's guidance. No application for hotline approval is needed.

Resources for Ireland:

www.dataprotection.ie/viewdoc.asp?DocID=303

Denmark

While Denmark has not adopted guidelines specifically addressing hotlines, it requires organizations operating hotlines in Denmark to register with the Danish data protection agency. The registration form, as well as a link to helpful guidance on how to complete the form, can be found on their website.

Resources for Denmark:

www.datatilsynet.dk/english/whistleblower-systems/

Sweden

Although a member of the EU, Sweden shares with Ireland and the UK a more welcoming approach to whistleblowers. This encouraged Wikileaks to move its servers there in 2007. However, Sweden's Personal Data Act reflects the data privacy principles in the EU's 1995 Directive, and the Swedish Data Inspection Board has applied the law to restrict whistleblower hotlines as follows:

Summary: Swedish Personal Data Act

1. The scope of the hotline is limited to financial and accounting issues, or other critical issues affecting the vital interests of the organization or the health and life of individuals
2. Use of the hotline should be voluntary, and it should supplement existing channels of communication
3. Only key personnel may be reported on through the hotline

Resources for Sweden:

ipandit.practicallaw.com/8-502-0348

www.linklaters.com/Publications/Publication1403Newsletter/20110119/Pages/06_Sweden_Registration_Provisions_Relaxed_Whistle_Blowing_Hotlines.aspx

GLOBAL ETHICS BY REGION:
Asia

Asian countries, with the exception of Hong Kong which follows the EU model, generally have little data privacy legislation. Taiwan, Singapore and Japan have enacted limited laws restricting data collection, for example, by government bodies, and giving individual rights of access. These laws are often aspirational and rely on self-regulation. However, APEC (Asia Pacific Economic Cooperation) which includes Canada, Australia and New Zealand, has launched an initiative to develop regional standards, and some proposals have been put forward. It is a contentious subject, as the component nations have very differing views on this subject.

Mainland China

No general data protection legislation.

Hong Kong

Hong Kong's Personal Data (Privacy) Ordinance is based on the EU Directive and accords rights of access and correction of personal data. Personal data collected, held or processed in Hong Kong may not be transferred outside Hong Kong unless the country to which it is transferred has similar privacy protection, or the subject consents. As The Network is Safe Harbor certified, transfer of data from Hong Kong is permissible.

Taiwan

The Computer-Processed Personal Data Protection Law concerns the collection and use by government agencies and some Taiwanese private sector bodies of personally identifiable information. The 1995 law requires that "collection or utilization of personal data shall respect the rights and interests of the principal and such personal data shall be handled in accordance with the principles of honesty and credibility so as not to exceed the scope of the specific purpose," with an "in principle" right of data access, correction and deletion. Data flows to countries without privacy legislation can be prohibited.

Singapore

In 1998 the government's National Internet Advisory Committee released an E-Commerce Code for the Protection of Personal Information and Communications of Consumers of Internet Commerce that embraces industry bodies. It limits collection and unauthorized disclosure of personal information; consumers have some limited rights regarding the restriction of data transfers and data correction/deletion.

Japan

In response to global financial scandals, and following the enactment of corporate governance legislation in other countries such as the Sarbanes-Oxley Act, the Japanese government enacted the Financial Instruments & Exchange Law. The law, commonly referred to as J-SOX (the Sarbanes-Oxley Act of Japan) provides for new rules for companies in regard to their internal financial controls. Japan's Financial Instruments & Exchange Law is therefore the equivalent of Sections 302 and 404 of SOX which also deals with internal financial controls and does not provide any guidance on employee complaint processes. J-SOX went into effect on April 1, 2008.

In June 2004, Japan passed the Whistleblower Protection Act. The Act affords employment protection to employees and impacts both the public and private sector. The Act requires a complaint to be investigated properly but has no penalties in place for corporations or government officials failing to do so.

With regard to data privacy protection, the national government has emphasized self-regulation by the private sector, especially regarding privacy aspects of electronic commerce, with a series of aspirational guidelines from the Ministry of International Trade & Industry (MITI) and other agencies. A suite of legislation passed in May 2003 established some general restrictions on the use and sharing of personal data, also giving individuals the right to obtain information collected by some private sector bodies.

Resources for Japan

www.fsa.go.jp/en/news/2007/20070420.html
www.thedeal.com/newsweekly/community/sox-in-the-land-of-the-rising-sun.php

India

No general data protection legislation.

GLOBAL ETHICS BY REGION:

South America

South America

Most South and Central American countries traditionally follow the “habeas data” approach to data privacy, emphasizing the individual’s rights to access and correct personal information in the possession of an organization. However, Argentina, Uruguay and Mexico have recently passed data privacy laws, similar to the laws passed by EU member countries pursuant to the EU’s Privacy Directive, in an effort to conform to EU data privacy principles and thus encourage trade with Europe. None of these privacy laws address whistleblower hotlines.

Broadly speaking, these laws restrict the use, retention or sharing of personal information (name, address, phone number, but also medical info, or any other sensitive personal information) beyond the narrow purpose for which it is gathered. They do not prohibit gathering such information if the subject consents, or in special circumstances such as the investigation of misconduct.

Like the EU, these EU-model privacy laws restrict the transfer of personal data outside their country to countries, including the U.S., which do not have such high standards of data protection.

Conclusion

An internal reporting program that supplements normal reporting procedures has proven to be a valuable tool in identifying corporate malfeasance and unethical behavior. The ability of multinational corporations to execute successful hotline/whistleblower reporting systems is critical, as studies have shown that employees are the best source for detecting corporate misconduct – better than either internal or external audits.

In addition, some countries, notably the U.S. with the Sarbanes-Oxley and Dodd-Frank Acts, require companies to provide confidential employee complaint mechanisms as a matter of law.

On the other hand, some countries restrict the implementation of whistleblower programs. The variance among different countries' regulations poses a tremendous challenge in today's global marketplace.

About The Network

The Network is an established leader in developing, managing and maintaining effective hotline programs for global corporations in countries around the world. The ability to tailor a program to specific legislation and guidance is a key element of The Network's success in supporting their clients' efforts in achieving and maintaining strong ethical culture and legal compliance.

The information and web links in this document are provided as a service to our hotline clients who want an introduction to some of the laws and regulations in the U.S. and elsewhere that affect hotlines. The Network is not a law firm and does not give legal advice. We recommend that you seek the advice of counsel in the appropriate area before implementing a hotline.

ABOUT THE NETWORK

The Network, Inc. is a leading provider of integrated GRC solutions that enable organizations to mitigate risk, achieve compliance and ultimately, create better, more ethical workplaces. Combining dynamic SaaS-based technology with expert-level services, The Network's Integrated GRC Solutions help companies around the world protect themselves from the risks posed by fraud and unethical conduct, detect issues early, and correct unethical or illegal behavior. Established in 1982, The Network serves thousands of organizations in every industry, including nearly half of the Fortune 500.

THE Network
Integrated GRC Solutions

For more information about The Network,
call 1-800-357-5137 or visit www.tnwinc.com