Whitleblowing Schemes: Best Practices and Implementation

Nick Ciancio
SVP, Marketing
Global Compliance
Nick.Ciancio@Globalcompliance.com
866-434-7009

Overview

- Review the goal to achieve SOX compliance and EU data protection principles
- Responsibilities to to make the process work
- Program insights
- Guideline reviews
- Recommended program approach

Global Compliance

Global Compliance

- Over 26 years of experience in ethics and compliance; Introduced the original reporting hotline in 1981
- Serves more than 2,000 clients including over 600 multinational corporations; provides services to more than 200 countries on behalf of our clients
- Most comprehensive and integrated product and services offerings of any provider in the industry
  - Awareness and Education
  - Information Intake and Management
  - Evaluation and Validation

Global Compliance

What is the Dilemma?

- SOX mandatory Code of Ethics

  A confidential, anonymous reporting mechanism

SOX Section 301(4) states that "Each audit committee shall establish procedures for the receipt, retention and treatment of complaints received by the issuer regarding accounting, internal accounting controls or auditing matters; and the confidential anonymous submission by employees of the issuer of concerns regarding questionable accounting or auditing matters."

Global Compliance

What is the Dilemma?

- E.U. data protection principles

- an individual has a right to know what data is being processed about them;
- personal data has to be processed fairly and lawfully;
- personal data must be kept for no longer than is necessary and must be accurate and up to date;
- each data subject has the right to know what or their personal data is being processed;
- personal data must be, at all times, kept secure and where processed by a third party be managed securely; and
- personal data should not be transferred outside the European Economic Area to any other country that does not have adequate protection for the rights of the individual.
- PLUS historical ethical and moral issues regarding “informers”.

Global Compliance

What is the Goal?

- Rigorous compliance with SOX
- “Substantial compliance” with E.U. data protection laws
  - Good faith compliance effort consistent with Art. 29 Working Party, CNIL and other guidelines

Global Compliance

What Will This Process Take?

- Real thought
  - Each company Code of Conduct / Ethics different
  - No quick knock-off or “one size fits all”
- Reconfigure E.U. whistleblower mechanism
  - New E.U. whistleblower protocol – without disturbing Code of Conduct / Ethics
    - New E.U. whistleblower procedure
    - New employee notice of whistleblower program
      - Usually requires translation
- Some companies doing procedure on pan-European basis
  - Slight adaptations by E.U. country where company has operations

Global Compliance

What Will This Process Take?

- Who makes this decision in your company?
  - Others' buy-in
- Who does the re-write?
  - Team
  - In-house counsel and staff, including compliance dept.
  - Outside counsel
    - In both U.S. and E.U. countries
  - Combination
- 3rd Party Vendor usage
  - Mechanisms – various levels of hotline / code of conduct interfaces and/or assistance
  - Contract terms – Required by Art. 29, CNIL, etc.
- Questions to data protection authorities
  - Member States differ
  - Some DPA's more accessible than others

Global Compliance

Issues

- Consider applicable laws for each EU entity
- Ensure that each EU entity is already notified with its DPA (if required)
- Ensure that staff contracts and staff manuals/handbooks address data protection and use of 3rd party providers
- Ensure that staff contracts and staff manuals/handbooks address whistleblower scheme
- Put in place contractual solutions to trans border data flows and controller to processor transfers
- Implement whistleblower policy and procedure for each EU entity

Global Compliance

Adapting Your Awareness and Education Program

- Code of Conduct
- Program Awareness (is ‘active promotion’ allowed?)
  - Allegation types
  - Reporting mediums (hotline, web, internal channels, Works Councils)
  - Anonymity
  - Whistleblower protection
  - Translations / local language
- Training and certification

Global Compliance

Program Implementation

- Provisioning phone lines
  - ITFS where available
  - Country-specific, in-language greetings and prompts
- Websites
  - Separate sites with country-specific text and instructions
  - In-language
- Allegation Categories
  - Broad versus narrowed financial-based
- Case Management
  - Permission-based functionality
  - Translation capabilities for case investigation and response to reporter
- Reporting
  - Transactional or summary reporting
  - Ability to segregate by country or enterprise-wide

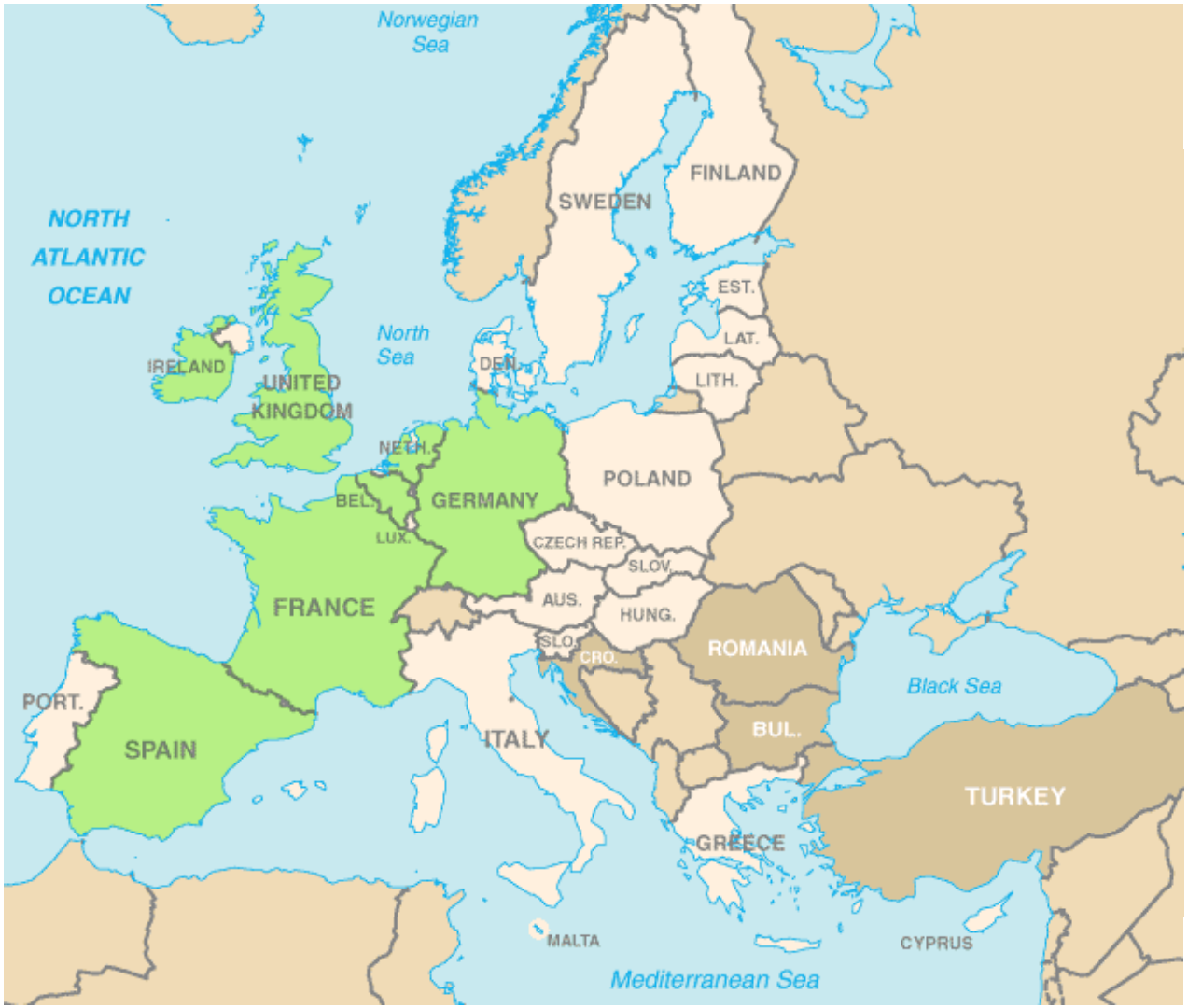
Global Compliance

Data Management

- Ability to block / restrict closed cases
- Ability to sanitize or delete specific information fields
- Permission-based access to specific information fields and to specific functionality within Case Management System

Global Compliance

EU Countries with Data Protection Guidelines



- United Kingdom
- France
- Germany
- Netherlands
- Belgium
- Ireland
- Spain

Global Compliance

France – CNIL Guidelines

- Whistleblowing system must be complementary
- Must be necessary to comply with legal obligation that requires it or necessary to realize data controllers legitimate interest; it doesn't override interests or fundamental rights of data subjects
- Legitimate interests: establishment of internal control procedures; internal control of credit and investments; to combat bribery; accounting and auditing matters
- Notification to CNIL (self-certification if system limited per the guidelines)

Global Compliance

EU Article 29 Working Party Guidelines

- Legitimacy – must be established to comply with a legal obligation (not a U.S. law) or necessary for legitimate interest of controller
- Data quality and proportionality – limit scope to minimum population coverage and minimize distribution of data
- Collect data for specific, identified purposes; ensure data accuracy; limit data retention; don't promote anonymous reports; preserve confidentiality
- Rights of incriminated person: information, access, rectification, erasure
- Security of data and operations; Safe Harbor of standard contract clauses; specific, dedicated organization

Global Compliance

Ireland - Irish Data Protection Commissioner Guidelines

- According to the Commissioner, "a best practice approach for an organisation introducing a whistleblowing scheme is to arrange, to the maximum extent possible, that the data produced from such a scheme refer to **issues** rather than **individuals**." By doing so, the organization would avoid capturing personal data and triggering the concerns of the EU Data Protection Directive.

- “Data controllers should follow the guidance contained in the [Article 29 Working Party's] Opinion [of February 1, 2006], otherwise they risk being found in breach of the Acts."

- Outsource data processing in compliance with EU requirements (standard contract clauses or Safe Harbor)

Global Compliance

Belgium Opinion

- Reporting mechanisms must be optional and should be limited to allegations of a serious nature such as crimes or rules violations (particularly with regard to finance and accounting)
- Allow only members of the organization to make reports or be the subject of reports
- Enable expedient notification of report subjects
- Use collected data for no other purposes
- Strict standards must be in place for compliant managers
- Confidentiality, availability, integrity, and authenticity of collected data must be ensured

Global Compliance

The Netherlands – Dutch Personal Data Protection Board (CBP) Opinion

January 2007

- Hotline can only be supplementary reporting channel
- Data transfer to parent company only if report relates to substantial abuses that exceed subsidiary level
- Cannot encourage anonymous reports
- Inform all employees about system; inform incriminated individuals
- Objective reports
- Reports must be handled within dedicated organizational unit
- Limit access to data
- Two-month retention
- Data transfer to parent company only if necessary

Germany – Dusseldorfer Kreis Guidance

April 2007

- Limited scope of allegations (reports relative to financial security in financial markets, prevention of fraud, accounting, internal accounting controls, auditing, bribery, banking and financial crime, insider trading)
- Allows anonymous reports
- Notification of incriminated persons, rectification rights
- Limited storage periods (2 months)
- Appointment of Data Protection Officer (DPO)
- No requirement to notify government agency if DPO appointed
- Right of co-determination (Works Councils)
- Must be voluntary
- Protect data subjects' rights

Global Compliance

Spain - Data Protection "Decision"

June 2007

- Limited scope of permissible allegations (conduct, actions or deeds that can constitute violations of internal rules of the company and of the laws, standards or ethical codes)
- Reports accepted by system must identify whistleblower; requires confidentiality of reports
- Data should be erased [deleted, blocked or archived] within a maximum of two months after the end of the investigations if the facts are not substantiated (data can be kept as long as necessary if legal proceedings are initiated)
- Notification of incriminated person (as soon as possible) of the facts reported, the recipients of the information, the department in charge of the system, and his/her rights with regard to data protection; Identification of the whistleblower will not be reported unless the person acted in bad faith
- High level security required under Spanish law

Global Compliance

Potential Difficulties of Spanish Decision

- Operational requirements described in the opinion could be difficult to implement
- Conflict with EU Data Protection Authorities and other member states in the EU
- The Spanish agency's position specific to anonymity being unacceptable would create considerable difficulty for companies that must comply with the Sarbanes-Oxley Act or for other reasons wish to allow the submission of anonymous reports

Global Compliance

Spanish Decision: Clarification Efforts

- Obtained in-country legal representation
- Letter sent to Spanish Agency stating concerns with the guidelines, lack of clarity, and conflict with SOX
- In-person meeting in Madrid, Spain on September 17, 2007 to seek clarification
- Working closely with Spanish agency to help define guidelines in order to craft the general decision
- Soliciting client participation to provide feedback and data to the Spanish Agency

Global Compliance

Information Needed for Spanish Agency

The Agency has asked Global Compliance and its clients to provide feedback regarding:

- Types of allegation received in anonymous reports
- How your company monitors the anonymous reports received
- Who monitors the hotline and reports received in your company
- How reports are received and managed within your organization; Who sees them
- How long are reports retained and where
- How long it normally takes for your company to complete its handling of an anonymous report
- What types of summary or management reports are prepared – and who receives them

Global Compliance

Program Approach

- Consider common guidelines across EU and make country-specific adaptations
  - Implement on a country-by-country basis
  - Establish separate programs when necessary to meet unique requirements
  - Pan-European or global solutions based on the most stringent country-specific requirements limit the effectiveness of the comprehensive program

Global Compliance