

Whistle-Blowing Hotlines  
under  
EU Data Protection Law

Suzanne Innes-Stubb

*Presented jointly by:*

**White & Case LLP**

*and*

**American Chamber of Commerce to the European Union**

# Agenda

1. Introduction
2. How does EU data protection law apply?
3. CNIL's Guidance and 'Single Authorisation'
4. Article 29 Working Party Opinion 1/2006
5. Scope of Opinion 1/2006 and Single Authorisation
6. Features of permitted whistle-blowing hotlines
7. Situation in other EU Member States
8. Conclusion

## 1. Introduction

- How can companies implement whistle-blowing hotlines in compliance with EU data protection law?
- Problem arose in May 2005 when French Data Protection Authority (CNIL) refused to authorise hotlines proposed by French subsidiaries of McDonald's and Exide Technologies
- CNIL particularly concerned about anonymous reporting and wide circulation of report within company before incriminated person informed
- Conflict with Sarbanes-Oxley Act in U.S.
- Revealed fundamental cultural differences
- Led to regulation in France and Opinion from Article 29 Working Party

## 2. How does EU data protection law apply?

- EU data protection law applies to individuals who are identified or identifiable from particular data
- Unless a whistle-blowing report is anonymous and no individual can be identified in connection with the matter raised in the report (unlikely), then 'personal data' will be involved
- Two data subjects: reporting employee and incriminated employee
- Obligations on the employer, as data controller, to carry out data processing lawfully, provide information to data subjects, ensure they have access to personal data, ensure security, etc.

### 3. CNIL's Guidance and 'Single Authorisation'

- CNIL issued stringent Guidance in November 2005 on the conditions for implementing whistle-blowing hotlines in compliance with French data protection law
- 'Single Authorisation' issued in December 2005
  - Requires company to self-certify on CNIL website that its whistle-blowing scheme complies with the Single Authorisation and Guidance
  - CNIL sends an acknowledgement of receipt which constitutes the authorisation
  - Schemes outside the scope of the Single Authorisation require individual CNIL authorisation (takes two months)
- FAQs issued in March – already updated

## 4. Article 29 Working Party Opinion 1/2006

- In other EU countries, data protection issues surrounding whistleblowing hotlines are primarily governed by an Opinion of the Article 29 Working Party (WP 29) in February 2006 (Opinion 1/2006)
- WP 29 Opinion based closely on CNIL guidance
- WP 29 Opinion is not legally binding but represents views of all DPAs in Europe, so carries considerable authority

## 5. Scope of Opinion 1/2006 and Single Authorisation

- WP 29 Opinion only applies to whistle-blowing hotlines necessary for
  - compliance with an EU or national legal obligation in the fields of accounting, internal accounting controls, auditing matters, or the fight against bribery, banking or financial crime, or
  - a legitimate interest (including compliance with foreign legislative requirements) in the same fields.
- CNIL Single Authorisation only applies to whistle-blowing hotlines
  - required by French law in the fields of finance, accounting, banking and bribery, plus Sarbanes-Oxley, or
  - where *"the vital interest of the company or the physical or moral integrity of its employees are at stake"*.

## 6. Features of permitted whistle-blowing hotlines

- Must not be the primary mechanism for reporting misconduct (and, in France, at least, must be optional)
- Anonymity must not be encouraged
- Data collected must be limited to the relevant facts
- Personal data must be deleted within two months of completion of the investigation, unless legal or disciplinary proceedings or national archiving rules require longer

## Features (cont.)

- **Company must tell employees:**
  - about the hotline and its purpose
  - how it works
  - who receives the reports
  - how employees can access, correct and delete incorrect information
  - that the identity of the reporting person will remain confidential
  - that action will be taken against individuals abusing the system
- **Company must give the incriminated person information about the report as soon as possible (once evidence has been secured if necessary)**

## Features (cont.)

- Data must be kept securely
- Reports must be made through a dedicated hotline
- Reports must be handled by specifically trained individuals subject to specific confidentiality obligations
- Particular obligations apply where whistle-blowing reports are processed by third party service providers

## Features (cont.)

- EU data transfer rules apply when either the service provider is located outside the EEA or the report is sent to other members of the corporate group outside the EEA
- Works council approval is required in a number of EU countries
- Notification to the national DPA is required; sometime prior approval is necessary

## 7. Situation in other EU Member States

- Most EU DPAs have no whistle-blowing rules or guidance and just refer to the WP 29 Opinion
  - Irish, Latvian and Spanish DPAs have limited website comments or information
- WP 29 Opinion represents views of all 25 EU DPAs, but underlying differences of approach to whistle-blowing hotlines:
  - Some countries focus more on whistle-blowers' rights (e.g. UK legislation, Dutch bill, Norwegian provisions not yet in force)
  - Belgium, Italy and Spain, in particular, likely to follow French approach and view anonymity with suspicion

## 8. Conclusion

- Where do companies stand now?
- Not clear whether SEC will accept that WP 29 Opinion, particularly regarding anonymity, will comply with Sarbanes-Oxley
- We recommend that European whistle-blowing hotlines follow the WP 29 Opinion as closely as possible
- But companies should be prepared to amend their schemes in particular countries if required by works councils or national data protection authorities
- French hotlines should comply with Single Authorisation.

Worldwide. For Our Clients.

[www.whitecase.com](http://www.whitecase.com)