Whistleblowing schemes were introduced in the EU as a result of the Sarbanes-Oxley Act (“SOX”) adopted by the US Congress in 2002 following various corporate financial scandals. SOX requires US companies and their EU-based subsidiaries to 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 of auditing matters”. Public companies which fail to put into place whistleblowing schemes may be subject to penalties provided by the Nasdaq, NYSE or the SEC. In addition, voluntary implementation of codes of conduct providing for whistleblowing schemes has become a relatively widespread practice amongst private companies, particularly international companies having entities in the EU.

The implementation of whistleblowing schemes will, in most cases, lead to the collection, processing and transfer of personal data (e.g., name of the accused person). Within the EU, personal data collection, processing and transfer is regulated by the Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the “Directive”). The Directive has been transposed into the national laws of all the EU national countries. In this regard, implementing whistleblowing schemes in
US companies’ European subsidiaries or branches will require compliance with EU data protection rules, with the risk of facing sanctions from EU data protection authorities if they fail to comply with such rules.

Whilst whistleblowing is not codified in the EU (there are no statutory obligations to implement whistleblowing schemes, nor any specific protection rules against retaliation of the whistleblower), whistleblowing procedures must comply with EU data protection rules provided by the Directive, and the national laws having implemented the Directive (i.e., the French Data Protection law\(^2\), the German Federal Data Protection Act (BDSG)).

**Legitimacy of Whistleblowing Schemes and Compliance with the Principles of the Directive**

In order to be lawful, whistleblowing schemes need to be legitimate and satisfy one of the reasons set out in Article 7 of the Directive, in order for personal data to be processed, such as compliance with a legal obligation to which the data controller is subject to\(^3\). Such obligations exist in most EU Member States: in the banking sector for example financial institutions are required to declare suspicious financial operations.

Personal data must be collected for specific, explicit and legitimate purposes and processed fairly and lawfully. Processed data must be adequate, relevant and not excessive in relation to the purpose for which they are collected and further processed. Appropriate measures need to be taken to ensure that data which are inaccurate or incomplete can be erased or rectified\(^4\). Finally, personal data must only be kept for the period of time strictly necessary for the purpose for which the data was collected or further processed.

Certain EU countries will also require that the company notify the existence of the whistleblowing scheme and data collection and processing with the local data protection authority.

**Compliance with Local Employment Laws**

Whistleblowing schemes within companies located in the EU must comply further with the requirements of local employment law. For instance, in France and in Germany, the employer must inform and consult the works council in advance of the implementation of whistleblowing schemes. A French works council will need to render a non-binding opinion, whereas in Germany, the employer and works council will need to agree on a works agreement to
implement a whistleblowing system because of co-determination rights.

Moreover, in most EU countries, employers may not require that their employees blow the whistle; they can only invite them to do so. Whistleblowing schemes in Europe will therefore need to be accordingly adapted.

**Rights of the Incriminated Person**

Whistleblowing schemes must guarantee the data subject’s rights, which means that the person accused in a whistleblower’s report must be informed when data concerning him/her is recorded. In particular, the accused employee must be informed of:

- the entity responsible for the whistleblowing scheme,
- the actions s/he is accused of and related facts,
- the department which may receive the report within the company or in other entities, and
- how s/he may exercise his/her rights of access, rectification and deletion.

Furthermore, anonymous whistleblowing is generally not permitted in many EU countries (evidence obtained from anonymous whistleblowing will be inadmissible), so that US companies will often need to modify the schemes slightly for their European entities.

Finally, the confidentiality of personal data must be guaranteed when it is collected, disclosed or stored.

**Clear and Complete Information about the Whistleblowing Scheme**

Employees must be provided with clear and complete information about the existence, purpose and functioning of the whistleblowing scheme, the recipient of the reports and their rights of access, rectification and erasure for reported person.

**Data Transfer Outside the EU**

Whilst data transfers within the EU would be permissible due to the harmonized level of protection throughout the EU Members State, cross-border data transfers, in particular to the US – which is not considered as a country providing an adequate level of protection in terms of personal data – must comply with the provisions of the Directive. In practice, such transfers will easily occur if the management of the whistleblowing scheme has been outsourced to a
service provider located in the US or if the US headquarters need to be informed of any alerts made by employees located in the EU.

In order to transfer personal data outside the EU, the data exporter located in the EU and the data importer (located outside the EU) will need to have put into place protective measures to permit the transfer of data and its protection, such as entering into a data transfer agreement based on the Standard Contractual Clauses approved by the EU Commission, adopting group-wide Binding Corporate Rules approved by the competent national data protection authorities or obtaining the individual data subject’s unambiguous consent; however, consent would not generally be permissible as a solution, as many Member States do not consider consent given in an employer-employee context to have been freely given.

As far as the US Department of Commerce Safe Harbor certification is concerned, the European Court of Justice’s decision in Schrems vs. Data Protection Commissioner invalidated the EU Commission’s decision recognizing Safe Harbor certification in its judgment dated October 6, 2015. The EU considered that Safe Harbor did not comply with the provisions and guarantees of the Directive on the protection of data, so for the time being, Safe Harbor is no longer a permissible solution. The use of the ECJ Commission approved Standard Contractual Clauses or the Binding Corporate Rules regime, also approved by the Commission, are still available to permit such transfers, as is explicit consent by the Directive on the protection of personal data subject to the data transfer (except perhaps in an employer-employee relationship).

For further information about this update, or if you have questions about Bryan Cave’s White Collar Defense and Investigations, Securities Litigation and Enforcement, Data Privacy and Security, or Labor and Employment practices, please contact Joseph Smallhoover or Sarah Delon-Bouquet.

---

1 Sarbanes-Oxley Act, Section 301 (4)  
2 French law n°78-17 dated January 6, 1978  
3 Article 7 (c) of the Directive  
4 Article 6 (1) (d) of the Directive  
5 Article 11 of Directive 95/46/EC  
6 Article 12 of Directive 95/46/EC  
7 Article 16 of Directive 95/46/EC
<table>
<thead>
<tr>
<th>RELATED PRACTICES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Privacy and Security Team</td>
</tr>
<tr>
<td>Securities Litigation and Enforcement</td>
</tr>
</tbody>
</table>