A Timely Analysis of Legal Developments

ASAP®

March 4, 2014

More CNIL Guidance for Multinationals Seeking to Comply with SOX & Dodd-Frank

By Philip M. Berkowitz, Philip L. Gordon, Michael G. Congiu and Lavanga V. Wijekoon

United States employers operating in France often face a dilemma. While they may be bound by the whistleblowing requirements of the Sarbanes-Oxley Act ("SOX") and its Dodd-Frank amendments,[1] they also are bound by the data privacy requirements of French law, which can be at odds with U.S. whistleblowing laws. The French data protection authority (La Commission Nationale de l'Informatique et des Libertés or "CNIL") periodically issues guidelines that provide some clarity on how employers can resolve this conundrum. On January 30, 2014, the CNIL finalized amendments to these guidelines[2] expanding the scope of the topics that could be disclosed through an anonymous whistleblowing hotline. The amendments also clarify the conditions under which SOX-type anonymous whistleblowing is permitted under French law.

Expansion of Topics of Anonymous Reports

Since 2005, employers operating in France must register their whistleblowing schemes with the CNIL. They may do so by self-certifying under the CNIL's Single Authorization (AU-004) that their whistleblowing scheme complies with the pre-established conditions set out in this authorization. Originally, the scope of the Single Authorization was limited to finance, accounting, banking, corruption, and compliance with Section 301(4) of SOX, which requires covered entities to establish procedures for employees' confidential and anonymous submission of questionable accounting or auditing matters, and the company's treatment of those reports. In 2010, the CNIL extended the scope to include the prevention of anti-competitive practices and compliance with the Japanese Financial Instrument and Exchange Act. The most recent amendments expand this scope further to cover certain non-financial topics, including workplace discrimination, harassment, safety, hygiene, and environmental protection.

---

1 The extra-territorial application of these U.S. laws is an open question. For more information on this subject, *see* Gregory C. Keating, *Whistleblowing & Retaliation*, Ch. 10 (International Whistleblowing Issues), 5th ed. 2013. *See also* Eric A. Savage, *Can SOX Go Overseas? The Debate Continues*, Littler ASAP (Feb. 19, 2014), available at http://www.littler.com/publication-press/publication/can-sox-go-overseas-debate-continues.

2 Délibération n° 2014-042 du 30 janvier 2014 modifiant l'autorisation unique n° 2005-305 du 8 décembre 2005 n° AU-004 relative aux traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle, CNIX1403184X, Jan. 30, 2014, *available at* http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=656E3F9168B3D0B618C7903416BB718B.tpdjo04v_2?cidTexte=JORFTEXT000028583464&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000028583033/.

The self-certification process is one of two methods of registering with the CNIL; the other is filing a formal request for approval with the CNIL—a more *ad hoc* process. The CNIL's expansion of the self-certification topics may indicate the authority's preference that employers use the self-certification process rather than the *ad hoc* process.

Newly Articulated Conditions for Anonymous Whistleblowing

The CNIL emphasized that the amendments, clarifying the conditions for anonymous whistleblowing, arise from its concern that anonymous whistleblowing increases the risk of slander in the workplace. Indeed, the CNIL has rejected whistleblowing schemes of companies where "the risk of slanderous denunciations" was, in its estimation, too great.[3]

The new guidelines attempt to balance the CNIL's interest in ensuring that employers establish a transparent whistleblowing system with its divergent interest in protecting the confidentiality of the report and the identity of the whistleblower. In particular, the guidelines require that a whistleblower self-identify, and that the corporate administrator managing the "alerts" treat that identification as confidential.

The CNIL also clarified that, under French law, anonymous reports are proper only in exceptional circumstances. For example, the report must be based on precise facts that are "serious" and the corporate administrator must screen the report to determine whether it may proceed through the whistleblowing system. Further, employers may not require or encourage employees to make anonymous reports.

CNIL Approval May Not Be Enough

Even if the CNIL certifies or approves an employer's whistleblowing scheme, a French court may still find that the scheme violates French law. For example, in 2011, a court of appeals in Caen struck down the whistleblowing scheme of a Michigan-based multinational's French affiliate *even though* the CNIL had certified that scheme under the Single Authorization.[4] The court held that, CNIL certification notwithstanding, a number of aspects of the scheme violated French law and the Single Authorization itself. This decision is a cautionary tale to employers that assume CNIL approval is sufficient to ensure their whistleblowing scheme is valid under French law.

Moreover, French courts may find the CNIL's newly expanded guidelines themselves violate French law. Indeed, in 2009, the CNIL was forced to rewrite its guidelines after the Court of Cassation—France's highest court—struck down guideline language that created an exception allowing employees to blow the whistle on issues not within the scope of the Single Authorization.[5] The exception allowed whistleblower reports as long as the vital interests of the company or the moral or physical integrity of the employees was at stake. The company involved in that case had expanded its whistleblowing scheme to require reports of sexual harassment and intellectual property violations. The court held that self-certified hotlines could not be broadened to breaches beyond subjects of finance, accounting or banking. Thus, employers should be aware of possible risks they may incur if they expand their whistleblowing schemes to include the CNIL's newly articulated topics for self-certification.

What to Expect and Consider

The CNIL's guidance provides useful clarity for employers that have implemented, or plan to implement, a whistleblower scheme that is consistent with French law. Despite this guidance, however, the area remains far from settled under French law and throughout several other jurisdictions in Europe. Though there is no substitute for enlisting the assistance of experienced counsel to navigate this fluid area of the law, we suggest the following:

- Closely monitor the CNIL guidelines and French law to ensure that a whistleblowing scheme comports with the topics and necessary conditions for submitting anonymous complaints.
- Institute a reporting scheme that offers anonymity, but does not require or encourage it.

---

3 *See Exide Techs.*, CNIL Decision no. 2005-111 (May 26, 2005); *McDonald's*, CNIL Decision No. 2005-110 (May 26, 2005).

4 *Benoist Girard (subsidiary of Stryker) v. CHSCT*, Cour d'Appel Caen 3rd Chamber (Sept. 23, 2011).

5 *CGT v. Dassault Systemes*, Court of Cassation—Social Chamber, Decision No. 2524 of December 8, 2009 (08-17.191).

- Confirm that the reporting scheme complies with the other procedural requirements in the CNIL's guidelines, such as provision of notice to the subject of the investigation and retention of documents related to the investigation for no longer than sixty (60) days after the investigation is closed unless the documents are needed for a disciplinary, administrative or judicial proceeding.
- To the extent feasible, rely on local employees to conduct the investigation and transfer personal data related to the investigation to the U.S. only if the U.S. parent corporation has implemented a mechanism for lawful cross-border transfers of personal data.
- Train and manage any corporate employees responsible for administering or monitoring a whistleblowing hotline.
- Oversee the operations of any third-party vendor that administers a whistleblower hotline.
- Maintain strict confidentiality regarding any complaints and/or investigations.

Philip M. Berkowitz, U.S. Practice Co-Chair of Littler's International Employment Law Group, is a Shareholder in the New York City office; Philip L. Gordon, Chair of the Privacy and Data Protection Practice Group, is a Shareholder in the Denver office; Michael G. Congiu is a Shareholder in the Chicago office; and Lavanga V. Wijekoon is an Associate in the Chicago office. If you would like further information, please contact your Littler attorney at 1.888.Littler, info@littler.com, Mr. Berkowitz at pberkowitz@littler.com, Mr. Gordon at pgordon@littler.com, Mr. Congiu at mcongiu@littler.com, or Mr. Wijekoon at lwijekoon@littler.com.