THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp
Editor, Kirk J. Nahra, CIPP
January - February 2011 • Volume 11 • Number 1

CNIL revises authorization on whistleblowing hotlines

By Olivier Proust

Initially, the French Data Protection Authority (CNIL) was reluctant to approve the use of whistleblowing hotlines within companies operating in France, as illustrated by its 2005 decision whereby it refused to approve the ethics hotlines set up by two companies on the grounds that the implementation of such schemes could create an organized process for corporate denunciation. That same year, however, the CNIL issued a single authorization AU-004 (autorisation unique) for the processing of personal data in the context of whistleblowing hotlines, which comprises a set of rules and guidelines explaining how to implement whistleblowing hotlines in France and what conditions apply to them.

On October 14, 2010, the CNIL adopted a series of amendments modifying and broadening the scope of its single authorization. The CNIL adopted these amendments after carrying out a consultation with private organizations, public institutions and authorities and works councils. While the CNIL's single authorization applies only in France, this amended version could foster amendments to whistleblowing regulations in other European jurisdictions and further discussions within the Article 29 Working Party.

In France, a whistleblowing hotline is considered to be a data processing activity that falls within the scope of the French Data Protection Act. Pursuant to Article 25 of the French Data Protection Act, "an automatic processing which may, due to its nature, importance or purposes, exclude persons from the benefit of a right, a service or a contract in the absence of any legislative or regulatory provisions" is subject to the CNIL's prior approval. For this reason, any company that intends to implement a whistleblowing hotline in France must first register this activity with the CNIL and obtain its prior approval. Companies have a choice between self-certifying to the CNIL's single authorization AU-004 or filing a formal application for approval with the CNIL. Its decision will largely depend on the scope of the scheme itself, as further explained below. While self-certification is a fairly straightforward procedure that does not require the CNIL's formal review, companies that register in this manner make a formal undertaking that their whistleblowing hotline complies with the pre-established conditions set out in the CNIL's single authorization AU-004. Failure to comply with these conditions, particularly if the scope of a whistleblowing hotline goes beyond what is authorized by the single authorization, creates a risk for companies that expose themselves to criminal sanctions.

If a company considers implementing a whistleblowing hotline that does not fully meet the requirements set out in the CNIL's single authorization AU-004, it must submit a formal application for approval to the CNIL describing

the whistleblowing scheme in detail, including the purpose of the data processing, the categories of data processed, the categories of data subjects, the data recipients, the data transfers and the security measures implemented. The CNIL carries out a case-by-case analysis of every application it receives, with particular attention paid to the intended purposes of the data processing activity and to the proportionality aspect with regard to the employees' privacy rights. After reviewing the applicant's request for approval, the CNIL issues a decision (délibération) authorizing or rejecting the processing activity. Since 2005, no more than 90 companies have received approval for their whistleblowing scheme in this manner, as opposed to 1,605 companies that chose to self-certify to the CNIL's single authorization.

The scope of the CNIL's single authorization AU-004 is limited to specific areas: finance, accounting, banking, fight against corruption and compliance with Section 301 (4) of the Sarbanes-Oxley Act. For example, a whistleblowing hotline may be used to report malfunctions within a company's accounting system, to combat bribery, tax evasion, falsification of official documents, false employment agreements, corruption of civil servants or to fight terrorism and money laundering. Under the CNIL's revised authorization, whistleblowing hotlines may also be used to comply with the Japanese Financial Instruments and Exchange Act and to prevent anti-competitive practices within the company. Regarding the latter, companies with anti-trust compliance procedures in place that include a duty to report possible anti-trust violations were previously required to obtain ad hoc approval by the CNIL. The CNIL's decision to extend the scope of its single authorization AU-004 to include anti-trust matters and to remove the burden of having to obtain ad hoc approval shows its willingness to accommodate companies that have an obligation to comply with both anti-trust and privacy laws in Europe.

Under the revised framework, the CNIL also deleted a former provision of the single authorization AU-004 that enabled companies to use their whistleblowing hotline exceptionally when "the vital interests of the company or the moral or physical integrity of the employees are at stake," even if the facts reported do not fall expressly within the pre-established scope of the single authorization. However, in a December 8, 2009 decision, the French Court of Cassation rejected that analysis and ruled that once a company has self-certified to the CNIL's single authorization AU-004, it cannot use its whistleblowing hotline beyond the pre-defined scope established by this single authorization. In this case, the Court of Cassation ruled that it was illegal for a company to use its whistleblowing hotline to report breaches of its Code of Business Conduct referring to a violation of intellectual property rights, disclosure of confidential information, conflicts of interest, insider trading, acts of discrimination and moral or sexual harassment. As a result, the CNIL deleted this exception from its single authorization, confirming that the scope of a whistleblowing hotline must be limited to the predefined areas, namely finance, accounting, banking, fight against corruption and anti-competitive practices and compliance with Section 301 (4) of the Sarbanes-Oxley Act and the Japanese Financial Instruments and Exchange Act. As a consequence, companies that self-certify to the CNIL's single authorization must inform their employees that any facts that are not expressly related to these areas must be reported by other means (i.e., manager, human resource department, trade unions).

Following these recent amendments, companies may consider whether it is appropriate to assess the level of compliance of their whistleblowing schemes with regard to French data protection law. Companies that have an existing whistleblowing hotline in France but have not registered it with the CNIL should consider doing so, particularly in light of the criminal sanctions that could be imposed by the CNIL (i.e., five years of imprisonment and a €300,000 fine) or, in case of litigation, by a court (i.e., French courts can multiply these criminal sanctions up to five times, amounting to a potential fine of €1.5 million). Companies that have already registered their whistleblowing schemes with the CNIL are not required to register them again. Nevertheless, the CNIL does expect them to amend their schemes, if needed, in order to comply with the revised single authorization AU-004.

These companies have up to six months, starting from the publication of the CNIL's revised single authorization AU-004, to do so.

Olivier Proust is an associate in Hunton & William's Global Technology, Outsourcing, and Privacy group. His practice focuses on all aspects of French and international data protection compliance projects, including implementation of global data management strategies, data transfers, and local data protection compliance. Proust also frequently counsels clients on various aspects of technology law, including privacy and security, e-commerce, and consumer protection. He is a member of the Paris Bar and the Brussels Bar E-List.