dataprotectionlaw&policy

FEATURED ARTICLE

cecile park publishing

Head Office UK Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND
tel +44 (0)20 7012 1380 fax +44 (0)20 7729 6093 info@e-comlaw.com
www.e-comlaw.com

French revised framework for whistleblowing: analysis

Last year, the French Data Protection Authority adopted a revised version of its single authorisation AU-004, concerning the processing of personal data in the course of whistleblowing procedures. Following the amendments, companies may consider it appropriate to assess the level of compliance of their whistleblowing schemes with French data protection law. Olivier Proust, Associate at Hunton & Williams, analyses the potential impact of the recently adopted revision on businesses.

The French Data Protection Authority (CNIL) adopted on 14 October 2010 an amended version of its single authorisation AU-004 ('autorisation unique') regarding the processing of personal data in the context of whistleblowing hotlines. The purpose of this revision was driven by two specific needs. On the one hand, the revised single authorisation broadens the scope of whistleblowing hotlines in response to the need expressed by companies to comply with corporate and anti-trust laws. On the other hand, it interprets more narrowly the conditions that apply to whistleblowing hotlines, in line with a decision of the French Court of Cassation, which ruled unambiguously that such schemes must necessarily be limited in their scope. The enactment of the Sarbanes-Oxley Act in 2002, and the rapid proliferation of whistleblowing hotlines within international organisations have compelled the European Data Protection Authorities to adopt a clear position regarding such schemes. The CNIL was at the forefront of the discussions that took place within the Article 29 Working Party, which eventually led to the adoption of an opinion on this matter. The CNIL officially addressed this issue in 2005, in two decisions involving the implementation by French subsidiaries of US companies of whistleblowing hotlines designed to comply with SOX. In these decisions, the CNIL indicated that the French Data Protection Act governs the set-up of whistleblowing schemes, since companies are able to collect and process personal data on their employees. In both cases, the CNIL refused to approve the hotlines set up by these companies on the grounds that their implementation could create an organised process for corporate denunciation. The CNIL considered the schemes to be disproportionate with regard to the risk of erroneous or slanderous workplace denunciation, and encouraged the companies to seek other methods for compliance with laws and company rules - for example, information and education initiatives, employee training, internal audits, reporting violations to an auditor or works inspector, civil or criminal actions.

That same year, the CNIL also issued a single authorisation (AU-004) for the processing of personal data in the context of whistleblowing hotlines, which comprises of a set of rules and guidelines explaining how to implement whistleblowing hotlines in France and detailing the conditions that apply to them. Pursuant to article 25 of the French Data Protection Act, whistleblowing hotlines are viewed as a system that can potentially exclude individuals from the benefit of a right, a service or a contract. 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 that implement a whistleblowing hotline in France have a choice between self-certifying to the CNIL's single authorisation AU-004 and filing a formal application for approval with the CNIL. The first option (self-certification) is a straightforward procedure that only requires companies to certify their compliance with the single authorisation AU-004. The CNIL does not formally review the whistleblowing scheme, but companies that register in this manner make a formal undertaking that their whistleblowing hotline complies with the pre-established conditions set forth in the CNIL's single authorisation. Failure to comply with these conditions - particularly if the scope of a whistleblowing hotline goes beyond what is authorised by the single authorisation - creates a risk for companies that exposes them to administrative and criminal sanctions. Alternatively, when a company's whistleblowing hotline does not strictly conform to the conditions set out in the CNIL's single authorisation, it must submit a formal application for approval to the CNIL, describing the whistleblowing scheme in detail - i.e. 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') authorising or rejecting the

processing activity. The chances of obtaining the CNIL's approval through this procedure are often slim, which explains why not more than 90 companies have received approval for their whistleblowing schemes in this manner since 2005, as opposed to 1605 companies that chose to self-certify to the CNIL's single authorisation.

Limited scope of whistleblowing hotlines

Whistleblowing hotlines cannot be used for general and unlimited purposes - such as to comply with all legal requirements, internal regulations and codes of conduct - since this would be considered disproportionate to the intended purpose. On the contrary, whistleblowing hotlines must necessarily have a pre-defined and limited scope. For this reason, they are considered to be lawful only when a French legal or regulatory provision requires companies to establish an internal control mechanism in specific areas - i.e., finance, accounting, banking, fight against corruption and anti-bribery. 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. In addition, companies that must comply with Section 301 (4) of SOX also have a legitimate purpose for implementing whistleblowing hotlines. Following a consultation with private organisations, public institutions and authorities, and works councils, the CNIL adopted several amendments to its single authorisation AU-004, which broaden the scope of whistleblowing hotlines. The revised single authorisation now refers to the Japanese Financial Instrument and Exchange Act - the so-called 'Japanese SOX' - and also states that whistleblowing hotlines may be used 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 authorisation 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.

The revised single authorisation now refers to the Japanese Financial Instrument and Exchange Act - the so-called 'Japanese SOX' - and also states that whistleblowing hotlines may be used to prevent anti-competitive practices within the company

Ruling of the French Court of Cassation

Prior to the CNIL's revision, companies could use their whistleblowing hotlines exceptionally to report facts that did not fall expressly within the pre-established scope of the single authorisation but nevertheless posed a serious threat to 'the vital interests of the company, or the moral or physical integrity of the employees'. In its decision of 8 December 2009, the labour chamber of the Court of Cassation struck down this provision on the grounds that, once a company has self-certified to the CNIL's single authorisation, it cannot use its whistleblowing hotline beyond its pre-defined scope. In this case, Dassault Systèmes had self-certified to the CNIL's single authorisation but then went on to expand its whistleblowing system to report serious violations of the company's Code of Business Conduct, such as violations of intellectual property rights, disclosure of confidential information, conflicts of interest, insider trading, acts of discrimination, and moral or sexual harassment. The Court rejected the company's argument according to which such use was permitted under the 'vital interests' exception, implying that it should have obtained the CNIL's explicit authorisation. As a result, the CNIL deleted this exception to clarify the scope of its single authorisation, thus confirming that whistleblowing hotlines must be limited to the pre-defined areas - finance, accounting, banking, fight against corruption and anti-competitive practices, and compliance with Section 301 (4) of SOX and the Japanese Financial Instrument and Exchange Act. As a consequence, companies that self-certify to the CNIL's single authorisation must inform their employees that any facts that are not expressly related to these areas must be reported by other means - for example, manager, human resource department, trade unions.

Companies which 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 - 5 years of imprisonment and a €300,000 fine - or, in case of litigation, by a court. 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 authorisation AU-004. These companies have until May 2011 to do so.

Olivier Proust Associate
Hunton & Williams
oproust@hunton.com