New EU Guidelines Prompt Review of Transatlantic Whistleblowing Schemes

Hanno Timner and Wim Nauwelaerts

On February 1, the Article 29 Working Party — an advisory body to the European Commission comprising member state data protection officials — adopted a long-awaited opinion with guidelines on how to implement whistleblowing schemes in Europe to comply with EU data privacy rules. These Guidelines were preceded by a sequence of events involving several unsuccessful attempts by multinationals to implement whistleblowing schemes in France and Germany. Before turning to the substance of the Guidelines, it may be useful to highlight the most important precedents in the EU so far.

The Compliance Dilemma

In the U.S., the Sarbanes-Oxley Act (SOX) (Section 301(4) in particular) and similar provisions in the Nasdaq and NYSE regulations require that publicly held companies and their EU-based affiliates, as well as non-U.S. companies listed in one of the U.S. stock markets, establish a system to allow employees to anonymously submit their concerns about a company's questionable accounting or auditing practices. Failure to set up a whistleblowing system may result in sanctions and penalties imposed by Nasdaq, NYSE or the Securities and Exchange Commission (SEC).

At the same time, companies face the risk of sanctions under applicable data privacy, labor or criminal law in the EU member states if their whistleblowing systems affect employees in those countries. In June 2005, the French data protection authority, the CNIL, issued two unfavorable rulings following its review of whistleblowing systems designed by McDonalds France and a local subsidiary of Exide Technologies, respectively. Both companies were told by the CNIL that they could not implement their whistleblowing schemes, as these would violate basic principles of French data privacy law and were therefore illegal. For completely different reasons but with a similar result, Wal-Mart was unable to implement an anonymous telephone hotline for its operations in Germany. The Higher Labor Court in Duesseldorf ordered Wal-Mart to withdraw its whistleblowing policy, mainly because Wal-Mart had failed to comply with mandatory rules on co-determination of its works council in Germany.

Wim Nauwelaerts

Hanno Timner

Saved by the Guidelines

The Article 29 Working Party has responded to industry's appeal for EU-wide legal certainty in this matter by adopting Guidelines that address the most urgent issues pertaining to whistleblowing schemes in the field of accounting and internal accounting controls, auditing matters, as well as the fight against bribery, banking and financial crime. The objective of the Guidelines is twofold: to give practical guidance to businesses and alleviate their concerns as to whether EU data privacy rules could frustrate the implementation of whistleblowing schemes in Europe.

The Guidelines focus on the admissibility of whistleblowing schemes designed to comply with SOX and similar regulations governing reporting of financial irregularities. The Article 29 Working Party intends to comment on the compatibility of whistleblowing schemes with EU privacy rules in other areas, such as human resources, workers' health/safety and environmental damage/threats, later this year. Although the Guidelines are not legally binding, their persuasive power is considerable, as they have been designed under the auspices of all national data protection authorities in the EU.

Main Principles for Guidance

The Guidelines set out two main principles that every whistleblowing scheme in the EU should respect. First, whistleblowing should be viewed as subsidiary to, and not a replacement for, internal management. The Article 29 Working Party shares the view of the French CNIL that the existence of whistleblowing systems can only be justified by the fact that conventional communication and reporting channels within an organization may not always be effective in all circumstances. This implies that companies should assess the implementation of reporting schemes that are less invasive from a data privacy perspective before implementing, for instance, anonymous hotlines for whistleblowers.

Second, whistleblowing schemes should only be implemented if they comply with applicable data privacy rules in Europe. According to the Article 29 Working Party, the rationale for this principle is that whistleblowing schemes pose serious risks of stigmatization and victimization of the person incriminated through such schemes. While existing

See ***New EU Guidelines,*** *page 10*

New EU Guidelines

continued from page 9

whistleblowing regulations typically include some degree of protection for whistleblowers, they do not focus on safeguarding the interests of the individuals incriminated under the system. Nonetheless, these individuals are entitled to protection under the EU Data Privacy Directive, as transposed into the EU member states' national laws.

Checkpoints for Compliance

To assess whether a whistleblowing scheme is compatible with EU data privacy rules, the Guidelines suggest that companies consider at least the following checkpoints:

- **Is the implementation of a scheme generally justified?**
  The processing of personal data in the context of a whistleblowing scheme must be justified generally by one of the legal grounds identified in the EU Data Privacy Directive. Relying on "compliance with legal obligations" seems to be the most obvious legal ground, at least at first sight. However, this is not an option if the whistleblowing obligations are imposed by rules applicable outside the EU, such as SOX. In those EU member states where mandatory national law does not require the implementation of local whistleblowing schemes, it may be possible for companies to invoke "pursuance of a legitimate interest" as a legal justification for processing personal data.

- **Are essential data privacy principles complied with?**
  Whistleblowing schemes should guarantee that all personal data is processed fairly and lawfully at all times, and that such processing is adequate, relevant and not excessive (proportionality principle). Furthermore, measures should be in place to ensure that the data is modified or erased when appropriate. In its Guidelines, the Article 29 Working Party highlights some of the practical ramifications that result from the application of these principles to whistleblowing schemes. For instance, as a rule, only identified, confidential reports should be communicated through the whistleblowing scheme. Anonymous reporting should be the exception to this rule, and the processing of anonymous reports should be subject to special caution (i.e., reports should be handled expeditiously, considering the potential risk of misuse). Another example involves data retention periods: personal data processed in the context of a whistleblowing scheme should be deleted promptly, usually within two months of completion of the investigation of the allegations. However, extended retention periods may be necessary if legal proceedings or disciplinary rules have been initiated.

- **Has there been clear and complete information about the scheme?**
  Before a whistleblowing system becomes operational, it is imperative that all relevant employees within the company's European offices are informed of the existence, purpose and functioning of the scheme, including who has access to whistleblowing reports. Employees should also be aware of the fact that a whistleblower's identity will be kept confidential throughout the process, although abuse of the system may result in sanctions.

- **Are the rights of the incriminated respected?**
  Whistleblowing schemes should be based on a careful balancing of interests, focusing on the rights of the incriminated individual, the whistleblower, as well as the company's legitimate investigation needs. Under the EU Data Privacy Directive, individuals incriminated through the scheme must generally be informed about the fact that allegations have been raised against them and that their personal data is being processed in this particular context. Furthermore, incriminated individuals should know that they have a right to access personal data relating to them and, potentially, to request correction or deletion of such personal data. It is noteworthy, however, that the Guidelines allow companies to delay the notification of an incriminated individual when there is a substantial risk that the investigation may be compromised if the individual is informed immediately. This possibility will need to be assessed carefully, on a case-by-case basis, to avoid circumstances that lead the individual in question to file charges for violation of data privacy rights. The incriminated employees must be informed of the entity responsible for the whistleblowing scheme, and the departments or services within the company that might receive the whistleblowing report. An incriminated individual has the right to object to the processing of his or her personal data, but the Article 29 Working Party takes the view that this right can be exercised only on compelling legitimate grounds relating to the person's individual situation.

> *"It is noteworthy, however, that the Guidelines allow companies to delay the notification of an incriminated individual when there is a substantial risk that the investigation may be compromised if the individual is informed immediately."*

- **Is the personal data processed securely?**
  Regardless of whether whistleblowing reports are collected electronically or in another form, all reasonable technical and organizational precautions should be in place to preserve data security. The Guidelines recommend that specific company resources should be dedicated to the whistleblowing scheme to enhance confidentiality and prevent diversion from its original purpose. If at any stage of a whistleblowing procedure, personal data is handled by exter-

nal service providers, contractual safeguards should ensure that such data processors adhere to adequate standards of security and confidentiality.

- **Is the scheme managed properly?**
  In the opinion of the Article 29 Working Party, companies should set up a specific internal organization for managing the whistleblowing scheme that is strictly separate from other departments, with specially trained and dedicated personnel. Alternatively, external service providers may be used, such as call centers, specialized companies or law firms to collect reports and/or conduct the necessary investigations. Since these service providers are considered data processors under EU data privacy law, it is essential to set up a contractual framework designed to cover the data flow from the service providers to the companies (which will be particularly relevant if, for example, several different law firms are involved throughout Europe). As a rule, multinationals are expected to deal with reports locally (i.e., in one EU country) rather than automatically share the data with other companies in the group, except when such communication is vital for the whistleblowing investigation.

- **Have possible data transfer issues been considered?**
  This question is relevant only to the extent that personal data gathered through a whistleblowing scheme is transferred to entities outside the EU. Since the European data protection authorities consider the U.S. to have inadequate protection of personal data, transfer of such data to the U.S. is subject to stringent restrictions. It will be up to the company to evaluate what would be the most suitable legal ground for transferring personal data to the U.S.: Safe Harbor-adherence, entering into contractual clauses with the recipient of the data, or binding corporate rules (provided they have been duly approved by the competent data protection authorities). As a measure of last resort, it may be possible to invoke one of the exceptional circumstances allowing transfer, as described in the EU Data Privacy Directive, but it is certainly not an option that the Article 29 Working Party favors (cf. "Transferring Personal Data Outside Europe: The Saga Continues," *The Privacy Advisor*, January 2006).

> *"... The Article 29 Working Party now has recognized that whistleblowing schemes can be useful tools to ensure compliance with rules of corporate governance, provided that principles of data privacy within the EU are respected."*

- **Has the scheme been notified/authorized?**
  The entity in charge of the whistleblowing scheme may be required to notify this particular type of data processing to the competent data protection authorities in some of the EU member states where personal data is collected. In some countries, notification may not suffice to comply with local data privacy rules if prior authorization is required. Companies planning to implement a whistleblowing scheme in the EU should be aware that compliance with these national notification/authorization requirements is often costly and time-consuming.

Toward More Legal Certainty?

The Guidelines bring a valuable contribution to the ongoing debate concerning the compatibility of whistleblowing schemes with the laws of EU member states. Focusing on aspects of data privacy only, the Article 29 Working Party now has recognized that whistleblowing schemes can be useful tools to ensure compliance with rules of corporate governance, provided that principles of data privacy within the EU are respected. At the same time, the Guidelines acknowledge that the application of data privacy rights (i.e., the right to information, access, rectification and erasure) may need to be restricted — at least to some degree — to balance the right to privacy against legitimate interests pursued by means of whistleblowing schemes.

At this point, however, a few caveats remain. First of all, the scope of the current Guidelines is restricted to whistleblowing schemes in the areas of accounting and internal accounting controls, auditing matters, and the fight against bribery, banking and financial crime. Additional guidance from the Article 29 Working Party on whistleblowing in other fields, such as human resources, is expected later this year. The present Guidelines are therefore provisional, to the extent that the Article 29 Working Party may adopt a final opinion on whistleblowing in general once it has a full understanding of all applications and data privacy issues involved. Whether such final opinion will suggest that national data protection authorities should adopt a "safe harbor" approach for whistleblowing schemes (as suggested by the French CNIL) remains to be seen.

Furthermore, the competent U.S. institutions and bodies (including the SEC) still are expected to confirm whether the Guidelines in fact enable companies dealing with whistleblowing schemes to comply with requirements imposed by SOX. On February 16, the Article 29 Working Party sent a copy of the Guidelines to Christopher Cox, Chairman of the SEC, inviting the SEC to further the transatlantic dialogue on the relevant issues to find common ground. To be continued, without a doubt.

Hanno Timner and Wim Nauwelaerts are attorneys in, respectively, the Berlin and Brussels' offices of Hogan & Hartson L.L.P., specializing in EU privacy and data protection law. They can be reached at htimner@hhlaw and wnauwelaerts@hhlaw.com.