Implementing a hotline for European operations: A single EU-wide approach or a country-centric design?

©2008 Steven A. Lauer
Corporate Counsel
Global Compliance Services, Inc.

In the United States, privacy is recognized as a legal, enforceable right only in certain specific contexts. Putting aside the area of criminal law,[1] Congress and the state legislatures have created a right to privacy only in respect of various types of information in relatively delineated sectors of society.[2]

This "sectoral" approach differs considerably from the approach taken in many other parts of the world. The European Union (the "EU"), for example, has enshrined "the right to protection of personal data concerning him or her" in its Charter of Fundamental Rights. Similarly, Asia-Pacific Economic Cooperation ("APEC") adopted a Privacy Framework that includes the recognition that "personal information protection should be designed to prevent the misuse of such information and the principles of notice, collection limitation, proper use of personal information, choice for the individual in respect of the collection, use and disclosure of his or her personal information, accuracy, security, access and accountability.

While that basic approach to personal information or data differs greatly between the United States, on the one hand, and much of the world community, on the other, even among the countries outside the United States, the approaches vary in many details. Those differences suggest some significant implications for business organizations' data-management activities, as a review of some of those differences, even among just countries within the EU, will demonstrate.

Actions by the EU regarding data protection and hotlines

To enshrine the status of privacy as a fundamental right, especially in light of recent technological advances, the EU enacted a directive (the "Directive") "on the protection of individuals with regard to the processing of personal data and on the free movement of such data."[3] The Directive adopted by the EU serves as the basis for the protection of "personal information" within the EU and provides direction to the member states of the EU as to how they should protect the fundamental "right to the protection of personal data" of their citizens.[4] Within the Directive, however, the EU also established a mechanism by which to provide more-specific direction to those member states through

---

[1] The Supreme Court has invalidated convictions on account of citizens' rights to privacy with respect to access to information about birth control, for example, in *Baird*.

[2] Congress enacted laws to protect personal health-related information (see the Health Insurance Portability and Accountability Act – known as HIPAA) and the financial-account information of consumers (see the Gramm-Leach-Bliley Act).

[3] See Directive 96/46/EC of the European Parliament of October 24, 1995, posted at http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

[4] The status of the efforts of the member states of the EU to implement the Directive's rules in their respective legal frameworks is summarized by the EU's agency for Freedom, Security and Justice in a document posted at http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm.

the creation of the Article 29 Working Party (the "Working Party"), the role of which is "to contribute to the uniform application of [national measures adopted under the Directive]."[5]

In that capacity, the Working Party has prepared a number of reports and decisions in which it has addressed various issues regarding the use and processing of personal information. In one opinion, the Working Party discussed how corporate whistleblowing mechanisms might be affected by the EU's data protection regimes and how the Directive and member states' implementing legislation would apply to whistleblowing mechanisms implemented by businesses.[6] In a distinct paper, the Working Party discussed the scope of the term "personal data."[7]

The Working Party's report on whistleblowing schemes provides a good window on the challenges facing corporate compliance and ethics executives in that the data-protection agencies of several member states have issued opinions, decisions and guidance documents on that topic since the Working Party's report appeared. What did the Working Party say in that report?

The Working Party limited Report WP117 to specific issues related "to the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime."[8] Because some EU member states' laws specifically provide for whistleblowing mechanisms while other states' laws include no specific provision for such a mechanism, the Working Party established what would constitute an acceptable justification for implementing a whistleblowing mechanism: "the purpose of meeting a legal obligation imposed by [EU] or Member State law, and more specifically a legal obligation designed to establish internal control procedures in well-defined areas." (Report WP117, p. 7.) According to the Working Party, "an obligation imposed by a foreign legal statute or regulation which would require the establishment of reporting systems may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate." (*Id*., at 8.) (The Working Party cited the Sarbanes-Oxley Act as an example of such a foreign law that would "not be considered as a legitimate basis for processing on the basis of Article 7(c)" of the Directive.)

The Working Party reviewed several principles established in the Directive and explained how, in its view, those principles would apply in respect of the processing of personal data that would apply to corporate whistleblowing schemes: fair and lawful processing, proportionality, and accuracy. In respect of proportionality, the Working Party indicated that "the company responsible for the whistleblowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistleblowing scheme" and "the company putting in place a whistleblowing scheme should carefully assess whether it might be

---

[5] See Article 30(1)(a) of the Directive.

[6] Rather than its somewhat unwieldy title ("Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime"), I'll refer to that report in this article, using its identifying number, simply as "Report WP117." The Working Party has posted the report at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf.

[7] See "Opinion 4/2007 on the concept of personal data" (document WP136), posted at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

[8] Report WP117, p. 4.

possible to limit the number of persons who may be reported through the scheme." (*Ibid*.)

The data quality principle requires steps to assure that the data collected and processed are accurate. Untrue or incomplete data must be erased or rectified.

The Directive also created specific rights on the part of an individual (a "data subject" in the lexicon of the Directive) whose personal data are collected and processed by a data controller. Those rights include not only a right to know that data concerning him or her has been or is being collected, but also to check the accuracy of the data so collected, to rectify it if inaccurate and to have it erased once outdated/

Actions by member states regarding data protection and hotlines

With the above actions (and others) by the EU as backdrop, let's examine how some EU member states have addressed questions regarding corporate whistleblowing hotlines. Have they created hurdles for multinational organizations operating in their respective jurisdictions? The short answer to that question is "yes," and an examination of a few issues will illustrate those hurdles. Specifically, the approaches that some countries in the EU have taken to the issues of (i) allowable allegations, (ii) the ability to accept reports that do not identify the caller/reporter and (iii) whether and how a subsidiary corporation can include its parent corporation in another country within the distribution of reports received over a hotline exemplify the challenges that such organizations face. Let's examine recent decisions or guidance documents issued by the data protection authorities of Belgium, France, Germany, Netherlands and Spain.[9]

The permissible scope of a whistleblowing hotline

The Directive states that personal data can be processed only for legitimate purposes and, with respect to a corporate hotline, the relevant purposes are that the "processing is necessary for compliance with a legal obligation to which the [data] controller is subject" and that "processing is necessary for the purposes of the legitimate interests pursued by the [data] controller … except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1)" of the Directive.[10]

None of the member states mentioned will accept satisfying the requirements of the Sarbanes-Oxley Act as a legitimate purpose for the collection and processing of personal information incident to the operation of a whistleblowing hotline. Rather, as suggested by the Working Party, they look to their respective organic laws to determine whether such a mechanism might be required within their jurisdictions and, if so, what the permissible scope would be. Unfortunately, those government agencies have reached disparate conclusions. What have they said?

Belgium: The Belgian Privacy Commission agreed with the Working Party that "a legal provision of Belgian law must be involved" to support the implementation of a whistleblowing system. Such a system "can only involve reports concerning problems

---

[9] Translations of the decisions discussed here can all be found on Global Compliance's website, at http://www.globalcompliance.com/legislation-knowledge-center.html.

[10] Directive Article 7(c) and Article 7(f).

that clearly would not be processed by the normal line of command and for which there is no specific procedure or body legally regulated." For issues not so described, the other, primary mechanism within the organization should be engaged. Because a whistleblowing system can only be a supplementary communication channel, reports must relate "to serious acts (violation of regulations applicable to the organization in question or internal written company rules (particularly in the departments of finance and accounting) or if a crime is involved," all of which means that it must involve "serious wrongdoing" or "serious facts or situations that must be reported in the general interest of the company or for the proper governance of the organization and for which the whistleblower considers it not or no longer possible through normal channels."

France: The Commission Nationale de l'Informatique et des Libertés (CNIL) issued guidelines in November 2005 "for the implementation of whistleblowing systems in compliance with the French Data Protection Act." CNIL identified a basis in French law for a whistleblowing system "relating to the internal control of credit and investment establishments" and for systems "whose purpose is to combat bribery." In France, as in Belgium, the whistleblowing system "must be designed as solely complementary to other reporting systems."

Germany: The German Ad Hoc Working Group on "Employee Data Protection" of the Düsseldorfer Kreis stated that a whistleblowing system is "intended as an additional mechanism for employees to report misconduct internally" and that it "supplement[s] the regular information and reporting channels." That working group identified the proper purposes of a system as the "goal of ensuring financial security in international financial markets," especially "the prevention of fraud and misconduct with respect to accounting, internal accounting controls, auditing matters, as well as the fight against bribery, banking and financial crime or insider trading."

Netherlands: In additional to the familiar litany of "accounting and auditing abuses," the Dutch Personal Data Protection Board referred to reports that "concern a substantial abuse" as among those that a whistleblowing system might accept, although it specified certain protections that an organization should implement with regard to ensuring that such reports are indeed so focused. A whistleblowing system also "cannot take the place of the normal handling options" for complaints.

Spain: In its opinion on reviewing the specifics of a whistleblowing system submitted for its approval, Spain's Agencia Española de Protección de Datos (AEPD) indicated that such a system should be "limited to reports involving internal or external topics or rules, the violation of which could have an actual impact on the maintenance of the contractual relationship between the company and the person incriminated." AEPD thus set out a somewhat broader scope of permissible allegations by tying that scope to the relationship between the organization and the party named in a report. Whereas other data protection authorities have expressed disapproval for reports of wrongdoing that does not relate to criminal violations,[11] then, AEPD seems to allow the receipt of a complaint over a

[11] For example, in it decision, the German Düsseldorfer Kreis stated that "[i]n the case of conduct which falls under [the phrase 'conduct which adversely affects company ethics'] ('soft criteria') the legitimate nature [of a report] can only be appraised on a case by case basis…. For this group … it is assumed that the legitimate interests of the data subjects [*i.e.*, individuals whose personal information appears in hotline reports and therefore is processed as part of the whistleblowing report] involved are compelling…. [A] connection between the breach and considerable loss for the company … cannot be identified so that at this point doubt arises as to the legitimate interest of the data controller [*i.e.*, the company]. Therefore in such

whistleblowing hotline so long as the subject matter of the complaint could serve as the basis for discipline of the data subject.

Caller anonymity

One issue that troubled the Working Party is the possibility that whistleblowing systems might receive anonymous reports. Whereas in the United States anonymity is an accepted – sometimes even encouraged[12] - protection for such matters, in Europe anonymity occupies a much less esteemed position. Indeed, according to the Working Party, "anonymous reports raise a specific problem with regard to the essential requirement that personal data should only be collected fairly. As a rule, the Working Party considers that only identified reports should be communicated through whistleblowing schemes in order to satisfy this requirement."[13]

To understand this view, you need to keep in mind the history of Western Europe. "In some Western countries such as France, Greece and Luxembourg, … whistleblowing is seen as little different from informing the government about a neighbor's dissident views. This, in turn, is frowned upon at least in part because it is considered an attribute of totalitarian or Communist states. In Germany, whistleblowing is thought unnecessary because of moral superiority."[14] The national data protection authorities expressed views very similar to that of the Working Party, but their decisions nonetheless create considerable challenge to multinational companies.

Belgium: Belgium's Privacy Commission "favors a general prohibition of anonymous reporting," although it then "subscribed to the argument developed by [the Working Party] that authorizes the processing of anonymous reports on a very restricted basis." The Commission outlined the procedural safeguards necessary to allow the receipt and processing of anonymous reports: absolute anonymity for the reporter, the need to conduct an initial investigation and reach a determination that the report contains well-grounded or baseless charges before any further dissemination within the company, such complaints must be processed by someone specifically appointed to handle complaints subject to professional obligations of confidentiality and with sufficient autonomy to insulate the processing from compromise and pressure from senior management, the need for utmost discretion in the processing of anonymous reports, and the obligation to cease processing a report if the confidentiality of the whistleblower has been intentionally violated.

France: CNIL expressed its belief that "[t]he possibility to file anonymous reports can only increase the risk of slanderous reports." Nonetheless, CNIL realized that "the existence of anonymous reports, even and especially in the absence of organized confidential whistleblowing systems, is a reality. It is difficult for company management

---

cases it can be assumed in principle that there is a compelling legitimate interest of the data subjects involved, and the processing or use of the personal data is not legitimate in this respect."

[12] See, for example, §301 of the Sarbanes-Oxley Act, which added a provision to the Securities Exchange Act of 1934 that requires corporate boards of directors to establish procedures by which employees could submit "confidential, anonymous submission[s] … regarding questionable accounting or auditing matters."

[13] Report WP117, at 11.

[14] Dworkin, "Whistleblowing, MNCs, and Peace," 35 Vanderbilt J. of Transnational Law 457, 470-471 (2002) (internal footnotes omitted).

to ignore this type of report, even when not in favour of them on principle." CNIL then delineated the need to have specific precautions for the handling of anonymous reports.

Germany: The Düsseldorfer Kreis agreed with the Working Party that anonymous reports should be accepted "only in exceptional cases." The group urged the protection of the identities of whistleblowers, with full information to those callers of the protection of identities in the system as a mechanism to discourage the filing of anonymous reports and the reduction in the need for them.

Netherlands: Personal Data Protection Board also recognized that "many reports are made anonymously and … it is not easy for many companies to deny such reports. The handling of these anonymous reports requires that special guarantees must be made, namely with regard to the first assessment of the report. An organization may not encourage the use of anonymous reports and must bring a system to life whereby the point of departure is that the identity of the informant is established. The reports themselves must be based on facts and not on individuals."

Spain: AEPD, in its opinion on the legality of a whistleblowing system submitted by an unnamed company for approval, quoted at length from Report WP117 on the acceptance of anonymous reports, even though disfavored and despite the advice required to be given to the caller. AEPD went on to say, however, that "procedures guaranteeing the confidential processing of reports filed through the whistleblowing systems must be established, so that the existence of anonymous reports is avoided" and that "[a]n initial filter of confidentiality and an additional possible final allegation of anonymity would not be sufficient for the operation of the system." The Spanish agency seems to prohibit even the acceptance of anonymous reports, then, which puts it squarely at odds with its counterparts in Belgium, France, Netherlands and Germany and the Working Party.

Transfer of hotline reports to a parent corporation in another country

With increasingly global business operations that span national borders and that involve multiple levels of corporate structure, corporate families often and regularly transfer data between and among related entities in the course of their business operations. To what degree do such transfers of data received through reports over a hotline implicate data transfer rules? How have the member states dealt with that issue?

The Working Party recognized the need for transfers between affiliated companies, such as from a company within the EU to a parent corporation outside the EU, even if that other country does not adequately protect personal information by law. The Working Party stressed that "the nature and seriousness of the alleged offense should in principle determine at what level, and thus in what country, assessment of the report should take place. As a rule, … groups should deal with reports locally … rather than automatically share all the information with other companies in the group." That Working Party did recognize, however, that "data received through the whistleblowing system may be communicated within the group if such communication is necessary for the investigation, depending on the nature of the seriousness of the reported misconduct, or results from how the group is set up.

Belgium: "Data transfers to a parent company in a country outside the European Union can only be justified if it involves particularly serious issues for which it has become obvious that the processing of the report cannot or can no longer be properly done

exclusively at the European organization level or that the processing may have repercussions beyond the company located in Belgium or in the European Union." Enterprise-wide compliance programs, then, would face hurdles in achieving enterprise-wide reporting and managing of allegations received through a whistleblowing mechanism.

France: CNIL recognized that, within a corporate family, "data received through the whistleblowing system may be communicated within the group if such communication appears necessary to the requirements of the investigation and results of the organization of the group. Such communication will be considered as necessary to the requirements of the investigation for example if the report incriminates a partner of another legal entity within the group, a high level member of management official of the company concerned." This may be a slightly more relaxed requirement than the Belgian one just cited. CNIL went on to warn, though, that "[i]f such communication appears necessary and the recipient of the data belongs to a legal entity established in a country outside the European Union which does not provide adequate protection [to personal information], the specific provisions of the EC Directive 95/46 of 24 October 1995 and of the French Data Protection Act of 6 January 1978, as amended, relating to international data transfers apply."

Germany: "The Düsseldorfer Kreis cited its general view that "[i]n principle it is not legitimate to transfer personal data of either the whistleblower or the incriminated person to third parties" and cited the transfer of such information in connection with further investigation of a report or with ensuing court proceedings as exceptions to that principle. Otherwise, that group did not address questions relating to intra-group data transfers.

Netherlands: The Dutch agency noted that "the forwarding of personal data to a third country may be appropriate" with appropriate safeguards regarding confidentiality. The agency's opinion provides no further detail regarding the appropriateness of transfers within a corporate group.

Spain: The AEPD discussed the transfer of personal data, received in hotline reports, to offices in other countries. With respect to transfers to countries outside the EU, AEPD stressed the need to use data transfer agreements, such as the EU-approved standard clauses.

Deletion or retention of data

The Directive provides that data "which permits identification of data subjects [must be kept] for no longer than is necessary for the purposes for which the data were collected or for which they are further processed."[15] The Working Party interpreted this to mean that "[p]ersonal data processed by a whistleblowing scheme should be deleted, promptly, and usually within two months of completion of the investigation of the facts alleged in the report."[16] What implications does that requirement hold for corporate hotline programs?

[15] See Article 6(1)(c) of the Directive.
[16] Report WP117, p. 12.

Belgium: The Belgian authority stated that the "complaint manager"[17] must "ensure that personal data … are kept for a period of time that does not exceed what is necessary for processing the report, including any legal or disciplinary procedures with regard to the person incriminated (in case of a justified report) or with regard to the whistleblower in case of unjustified reports or libelous accusations."[18]

France: CNIL took a similar view: "[d]ata relating to a report found to be unsubstantiated … must be deleted immediately" and "[d]ata relating to alerts giving rise to an investigation must not be stored beyond two months from the close of verification operations unless a disciplinary procedure or legal proceedings are initiated against the person incriminated in the report of the author of an abusive report."

Germany: The Dusseldörfer Kreis agreed that "data should be destroyued within two months after conclusion of the investigation" and that "[s]toring data for a longer period may only be legitimate until further legal measures … have been clarified." As to data included in an unsubstantiated report received over the hotline, however, that group determined that the data "have to be deleted without undue delay," a slightly different formulation than that used by the Belgian and French authorities.

Netherlands: The Dutch Personal Data Protection Board agreed with the two-month limit on data retention for concluded investigations , subject to longer a period for data if "disciplinary measures were taken against the informant (false reporting) or the person on whom the report was made (justified reporting)." As for an unjustified report, "[t]he processing … must be immediately suspended and the data destroyed."

Spain: AEPD quoted the Spanish data protection law as follows: "personal data shall be erased when they have ceased to be necessary or relevant for the purpose or which they were obtained or recorded." Thus, under Spanish law, "it would be essential for a maximum term to be established to preserve data related to the reports, in order to prevent the data from being kept for a longer period that could prejudice the rights of the incriminated person and also those of the whistleblower."

Where does this leave you?

To a large degree, the protections for personal data represented in the Directive and the clash between the views of EU data protection regulators and their U.S. counterparts reflect their countries' very disparate histories. The Working Party alluded to this in its opinion when it said the following:

> The number of issues raised by the implementation of whistleblowing schemes in Europe in 2005, including data protection issues, has shown that the development of this practice in all EU countries can face substantial difficulties. These difficulties are largely owed to cultural

[17] Under Belgian law, "[t]he report must be collected and processed by a person in the organization specifically appointed to hear complaints," who must be "bound to professional confidentiality when processing the report, even with regard to executives (unless immediate precautionary measures are required), other members of the staff, labor union organizations and third parties." See page 5 of the opinion of the Belgian Privacy Commission.

[18] *Id.*, at 6-7.

> differences, which themselves stem from social and/or historical reasons that can neither be denied nor ignored.[19]

The Chairman of the Working Party described those differences somewhat more explicitly in a letter to the Director of the Office of International Affairs of the Securities and Exchange Commission: "anonymous reporting evokes some of the darkest times of recent history on the European continent, whether during World War II or during more recent dictatorships in Southern and Eastern Europe. This historical specificity makes up for a lot of the reluctance of EU Data Protection Authorities to allow anonymous schemes being advertised as such in companies as a normal mode of reporting concerns."[20] We thus face very different views of the value of whistleblowing: in many countries within the EU, that technique conjures up images of "denunciation" as practiced in Nazi Germany or wartime France, while in the United States it evokes "Deep Throat" of Watergate renown.

For that reason, the implementation of a whistleblowing hotline in an organization with European operations must be well-planned. An effective awareness campaign by which the employees learn about the hotline occupies an essential place in that implementation, and not simply to satisfy the expectations of EU data protection regulators regarding how such a mechanism is "positioned."[21] That campaign should take into account the various requirements of EU regulators summarized above (as well as others).

In addition to such an awareness campaign, an organization that plans to implement a hotline should also consider training. Should the implementation of the hotline be accompanied at the same time, or at least relatively contemporaneously, by training on one or more topics relevant to the hotline? For example, if the organization will allow employees to use the hotline to report issues or concerns relative to accounting, auditing and similar issues consistently with the guidance issued by CNIL and the other EU member states discussed above, it might wish to provide its employees guidance on how to recognize such issues. A course on financial integrity or on what information might suggest financial irregularities or fraud has taken place could add considerable value to the hotline as part of a fraud prevention program.[22]

The variation of the data-protection requirements discussed above obviously presents hurdles for an effective implementation of a hotline for multiple countries within the EU. The scope of permissible allegations among EU member states, for example, represents one challenge to a multijurisdictional program. The ability to receive anonymous reports within the various countries also varies considerably.

One possible approach is to adopt what some call a "pan European" solution. An organization following this approach will design its program to meet the most stringent (from the perspective of the implementing organization) regulations among the EU regulators. For example, because the permissible allegations under CNIL's approach are

---

[19] Report WP117, p. 4.

[20] See page 3 of the letter dated July 3, 2006, by Peter Schaar, Chairman of the Working Party, to Ethiopis Tafara, posted at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2006-07-03-reply_whistleblowing.pdf.

[21] According to CNIL, for example, "[c]lear and complete information on the system must be given to potential users by any appropriate means." Other EU regulators have expressed similar views.

[22] See Lauer, "Compliance Programs And Fraud Prevention," The Metropolitan Corporate Counsel, vol. 14, no. 5 (May 2006), p. 61.

at least as narrow as those allowed by other member states' data protection authorities, allegation scope aligned with CNIL's guidance should suffice. By prohibiting the acceptance of anonymous reports, a company would satisfy the expectations expressed by AEPD in its June 2007 opinion.

This approach also carries, however, a significant risk. It works so long as the stringent standard on which it is based remains the most stringent standard. If any one or more jurisdictions issue guidance even more stringent on a substantial issue, however, the entire EU-wide program would require amendment. Had a program designed prior to June 2007 accepted anonymous reports as permitted by the Working Party, CNIL and other regulators, the Spanish decision would have affected that program's ability to accept anonymous reports anywhere within the EU.

For these reasons, flexibility has become an indispensable characteristic of an effective hotline. Country-specific regulations call for country-specific program design. While meeting the varying expectations of EU data protection regulators requires close analysis of their respective laws and guidance documents, once that analysis is complete for a country, it remains accurate for that country until that country's regulator changes its standards.