PROSKAUER ROSE LLP®

Whistleblowing Hotlines in Europe Under Sarbanes-Oxley:

Directions Through the Maze

International Labor & Employment Counsel
Proskauer Rose LLP, New York City

Perhaps, in this first decade of the millennium, the chief theme of multinational business operations is "compliance." In our post-Enron world of whistleblowing, white-collar crime enforcement, EU data protection, the OECD anti-bribery convention, U.S. Sarbanes Oxley [SOX], and all the rest, multinationals take their legal responsibilities one way: seriously.

Among those multinationals listed with U.S. stock exchanges, compliance with *SOX* surely tops the legal compliance agenda. SOX is of course a complex statute with broad ramifications in accounting and securities registration, and entire books have been written about how to comply with it. Additionally, a discrete, if thin, slice of SOX compliance raises unique problems of *international employment law:* The intersection of SOX's mandate for employee "complaint" "procedures" with European labor and data privacy laws.

One short provision in SOX tells the audit committees of listed multinationals to set up "complaint" "procedures" to root out ("recei[ve]" word of) wrongdoing. But specific applications of continental European labor and data protection laws insulate the *victims* of whistleblowing complaints—the alleged wrongdoers. These European doctrines challenge the legality of American-style hotlines launched to comply with SOX.

Since the summer of 2005, this sub-issue of SOX law has loomed as a storm cloud threatening compliance-focused SOX-regulated multinationals. Fortunately, the inconsistent U.S. and European legal doctrines may now be reconcilable. But they are a tight fit. To comply with them simultaneously, SOX-regulated multinationals need to adopt—and follow through on—a creative strategy. Forming this strategy requires a careful analysis of five discrete issues:

(1) SOX hotline law, and its extraterritorial reach

(2) SOX friction in Europe socially

(3) European works council labor law on "information and consultation" and co-determination with workers

(4) French data privacy law on whistleblower hotlines

(5) opinion of the EU "Article 29 Working Party" on the EU's probable position extending the French analysis more broadly in Europe

After examining each of these five issues, this article discusses six theoretical "best practices" strategy options for launching a SOX whistleblower hotline in continental Europe consistent with the legal constraints.

1. SOX Hotline Law, and Its Extraterritorial Reach

To understand why SOX hotlines raise tough European legal issues, we first must understand what SOX does—and does not—require as to hotlines, both stateside and abroad. The Sarbanes-Oxley Act of 2002, at § 806, protects from *retaliation* certain whistleblowers at companies listed or filing with U.S. stock exchanges, be the companies headquartered in the U.S. or abroad. Further, SOX § 301 affirmatively encourages whistleblowing by requiring the audit committees of SOX-regulated companies to institute "procedures" for handling "confidential, anonymous" "employe[e]" "complaints" and "concerns" over possible corporate misdeeds "regarding questionable auditing or accounting matters":

> Each audit committee *shall* establish *procedures* for: (A) the receipt, retention, and treatment of *complaints* received by the issuer regarding accounting, internal accounting controls, or auditing matters; and (B) the *confidential, anonymous* submission by employees of the issuer of concerns regarding *questionable accounting or auditing matters.*[1]

This § 301 is the only provision in SOX or SOX regulations that tells companies how to implement employee (as opposed to "senior financial officer" and attorney)[2] whistleblower hotlines/reporting procedures. In fact, when the SEC adopted its Rule 10A-3 under SOX § 301,[3] the SEC affirmatively *declined* to spell out hotline details, so as to give individual audit committees flexibility to develop their own procedures.[4]

Because § 301 merely requires: (A) "treatment" "procedures" for complaints received from anyone, and (B) "confidential, anonymous . . . employe[e]" "concern" "procedures," § 301 does not mandate hotlines *per se*. Nor does SOX mandate that employers force employees to report their fellow co-workers' violations. Hotlines and mandatory reporting rules are a SOX "best practice" within the U.S. and are encouraged by U.S. sentencing guidelines (and, under SOX, "promot[ing]" mandatory reporting is necessary for "senior financial officers" and attorneys).[5]

---

[1] Sarbanes-Oxley Act of 2002, Pub. L. 107-204, at § 301(4) (emphasis added). *See generally* SEC Rule 10A-3(b)(3); NASDAQ Rule 4350(d)(3); NYSE Listed Company Manual § 303A(6). Even though SOX § 301 deals primarily with accounting and auditing, the language "regarding questionable accounting or auditing matters" does not limit complaint "procedures" to auditing and accounting. Accordingly, "best practices" U.S. companies (in particular, those accounting for U.S. corporate sentencing guidelines) commonly institute procedures by which employees can report any corporate fraud or misdeed or ethics violation. But this is not a SOX requirement. As to sentencing guidelines, *see infra* note 5.

(As to the "audit committee" reference in SOX section 301, other sections of SOX require an issuer company to establish an independent audit committee responsible for overseeing the work of any registered public accounting firm employed by the issuer, and each accounting firm must report directly to the audit committee. *See id.* § 301(2).)

Further, SOX § 404 requires control systems to ensure listed companies can make adequate, SOX-mandated disclosures; this requirement may be read as an indirect requirement for whistleblowing systems consistent with SOX § 301. *See also* SEC Rules 13a-15; 15d-15.

[2] Section 406, the only other provision of SOX that regulates ethics codes and compliance codes generally, requires SOX-regulated companies to disclose whether they have adopted a code of ethics that applies to their "senior financial officers," including the principal executive officer, principal financial officer, comptroller or principal accounting officer, and "persons performing similar functions." SOX § 406(a) (emphasis added). *See also* Disclosure Required by Sections 406 and 407 of the Sarbanes-Oxley Act of 2002, Rel. Nos. 33-8177 and 34-47235 (Jan. 23, 2003), 68 Fed. Reg. 5109 (Jan. 31, 2003), *available at* http://www.sec.gov/rules/final/33-8177.htm (adding principal executive officer to the list of senior financial officers when the SEC adopted § 406 of SOX); SEC Item 406 of Reg. S-K; NASDAQ Rule 4350(n); NYSE Listed Company Manual § 303A(10).

Even this SOX section 406 codes-of-ethics rule does not mandate any company rule requiring senior financial officers to report corporate misconduct. Companies only need to "promote" this reporting. The SEC rule that adopts section 406 defines "code of ethics" to mean "such standards as are reasonably necessary to promote...(4) [t]he prompt internal reporting of violations of the code to an appropriate person or persons identified in the code." *See* Disclosure Required by Sections 406 and 407 of the Sarbanes-Oxley Act of 2002, Rel. Noxes. 33-8177 and 34-47235 (Jan. 23, 2003), 68 Fed. Reg. 5109 (Jan. 31, 2003), *available at* http://www.sec.gov/rules/final/33-8177.htm (emphasis added). Again, this "promote…internal reporting" language reaches only senior financial officers, and does not mandate that ethics codes force the senior financial officers to report corporate misconduct (i.e., § 406 does not require mandatory reporting rules even for senior officers). However, the SEC, as directed by SOX § 307, does require *attorneys* to report violations of securities law. *See* 17 C.F.R. § 205.3 (implementing SOX § 307).

This article on employee compliance measures abroad assumes overseas workforces will not employ "senior financial officers" or attorneys at this SOX section 406 and 407 level. That is, the analysis in this article focuses on employee populations abroad without regard to overseas "senior financial officers" or attorneys.

[3] The SOX statute required the SEC to adopt rules implementing certain provisions of SOX, including § 301.

[4] In its regulation adopting § 301, the SEC said: "As proposed, we are not mandating specific procedures that the audit committee must establish.... Given the variety of listed issuers in the U.S. capital markets, we believe audit committees should be provided with flexibility to develop and utilize procedures appropriate for their circumstances." 2003 SEC Lexis 846 at 68-71. The SEC also said it had considered but rejected a "one-size-fits-all model." *Id.*

[5] SOX § 406 merely requires companies to "promote"—not require—reporting among "senior financial officers." SOX § 307 and 17 C.F.R. § 205.3 *do* require reporting, but only by "attorneys," not by others. *See supra* note 2. Hotlines and mandatory reporting rules, within the U.S., are a "best practice" because they can help a company find out about fraud, and are consistent with U.S. sentencing guidelines. U.S. sentencing guidelines give credit, in "sentencing of organizations," to those "organizations" that establish "an effective compliance and ethics program." United States Sentencing Commission, *Guidelines Manual*, §8B2.1. But the sentencing guidelines do *not* speak to whether multinational "organizations" must extend that "program"

But our SOX hotline question here is *international*: Whether SOX mandates that these "confidential, anonymous" employee reporting "procedures" be available to employees of SOX-regulated companies (and subsidiaries) *who work and live abroad*. Unfortunately, SOX is unclear and unsettled on this point.[6] But, contrary to assumptions of many multinationals examining this issue, an argument exists that the SOX "complaint... procedure" mandate is confined stateside.

Like the rest of SOX, § 301 applies to "issuers" as defined in the Securities Exchange Act. Some issuers, foreign private issuers, are actually based overseas. Other issuers are based in the U.S. but have extensive employment operations abroad.[7] The SEC sees SOX as reaching foreign private issuers—the SEC even extended their date for SOX compliance.[8] To this extent, aspects of the Securities Exchange Act, and SOX, do apply abroad.

For this reason it is widely assumed that SOX's § 301 hotline ("complaint" "procedures") mandate applies abroad, as well. In fact, the SEC itself appears to assume this. In promulgating rules under § 301, the SEC implied that § 301 reaches U.S. based multinationals' *overseas employees*:

> The [reporting/hotline] procedures that will be most effective to meet the requirements for a very small listed issuer with few employees could be very different from the processes and systems that would need to be in place for large, *multi-national corporations with thousands of employees in many different jurisdictions.*[9]

The fact that the SEC appears to assume § 301 reaches overseas is hugely relevant to any multinational contemplating the scope of its § 301 hotline or "procedures." But an implicit position of the SEC is far from a settled point of law. Would a court really hold SOX § 301 reaches abroad?

Maybe not. Nowhere does the text of SOX § 301 say it reaches overseas employees. And this silence, under law, could itself mean it does not. Under a Supreme-Court-endorsed and widely-upheld canon of statutory construction, all U.S. federal statutes are confined to U.S. soil except for those in which, in their texts, U.S. Congress expressly manifested a clear "contrary intent" to reach overseas.[10] In *EEOC v. Arabian Am. Oil Co.*,[11] the U.S. Supreme Court held:

> Congress has the authority to enforce its laws beyond the territorial boundaries of the U.S.… Whether Congress has in fact exercised that authority [as to any given federal statute] is a matter of statutory construction. It is *a long-standing principle of American law* that legislation of Congress, *unless a contrary intent appears*, is meant to apply only *within the territorial jurisdiction of the United States*. This canon of construction serves to protect against unintended clashes between our laws and those of other nations which could result in international discord.[12]

In January 2006, a U.S. federal appeals court invoked this canon in a SOX whistleblower context, and held SOX's whistleblower retaliation provision, § 806, does *not* reach overseas employees. In *Carnero v. Boston Scientific Corp.*,[13] an employee claimed a SOX-regulated company had fired him for reporting accounting infractions. He sued for reinstatement and back pay. But this employee was an Argentine working for the company in South America. Because SOX § 806's retaliation provision says nothing about overseas application, the U.S. First Circuit Court of Appeals held the suit had to be dismissed: The SOX § 806 whistleblower retaliation provision simply does not reach abroad, because Congress never said it does.

---

abroad. *Id.* Also, the guidelines encourage *but do not require* confidential, anonymous hotlines: The "organization *shall* take reasonable steps to have and publicize a system, which *may* include mechanisms that allow for anonymity or confidentiality, whereby the organization's employees and agents may report...potential or actual criminal conduct without fear of retaliation." *Id.* at §8B2.1(b)(5)(C) (emphasis added).

6 There is very little case law on SOX § 301, and none of it addresses this question.

7 See JOHN T. BOSTELMAN, THE SARBANES-OXLEY DESKBOOK, § 3:2. Section 301 prohibits the listing of "any security of an issuer that is not in compliance with the requirements of" Exchange Act §§ 10A(m)(2)-(6). Thus, the scope of § 301 appears to turn on a company's status as an "issuer," which would appear to include all SOX-regulated multinationals—and § 301 does not distinguish multinationals' domestic-U.S. operations from their overseas operations. Exchange Act §10A(m)(4), 15 U.S.C.A. §78j-1(m)(4), *as added by* Pub. L. No. 107-204 § 301.

8 SEC Rule 10A-3(m), 17 C.F.R. § 240.10A-3(a)(5).

9 SEC Act Release No. 33-8220 (Apr. 9, 2003), 2003 SEC Lexis 846, at 71 (emphasis added). This language, however, does not clarify whether these "many different jurisdictions" include jurisdictions *overseas*. The SEC also appears vaguely to have taken the position that § 301 reaches abroad at SEC Act Release No. 33-8220 (4/9/03).

10 *See EEOC v. Arabian Am. Oil Co.*, 499 U.S. 244 (1991) ("Aramco"), *superseded in other respects by* 42 U.S.C. §§ 2000e(f), 12111(4). *Aramco* on this point is still good law; the Supreme Court cited it with approval in June 2005, in *Spector v. Norwegian Cruise Lines,* 125 S. Ct. 2169 (2005).

11 *Id.*

12 *Id.* at 248 (emphasis added). The "unintended clashes" with " laws…of other nations" and "international discord" issue is an enormous concern as to SOX § 301 hotlines, given the European Union labor and data privacy law doctrines discussed *infra*.

13 433 F.3d 1 (1st Cir., Jan. 5, 2006).

SOX § 301, which like § 806 is a SOX whistleblower law, is every bit as silent on extraterritorial reach as is § 806. So the *Carnero* analysis might apply to § 301—meaning that SOX "complaint" "procedures" may not be mandated overseas.

This conclusion, though, seems to trouble multinationals and some lawyers, who argue that this analysis cannot possibly be right. SOX § 301 differs from SOX § 806, they argue, because § 301's mandate to set up employee hotlines is less employment-law-related than is § 806's prohibition on retaliation—and, somehow, the canon restricting statutes to U.S. soil might apply more forcefully to employment laws than to hotline-mandate laws.[14]

This distinction finds a bit of support in dictum in the *Carnero* opinion itself: *Carnero* notes that SOX § 301 "does not…purport to confer enforceable rights upon employees, hence does not implicate the foreign sovereignty and other concerns [of §] 806…."[15] But this *Carnero* dictum may lose force in light of the fact that a fierce "foreign sovereignty" conflict is now raging between SOX § 301 and European Union data and labor laws.[16] Further, the case law supporting the canon of construction is not confined to employment cases. Therefore, a SOX-regulated multinational might conceivably rely on *Carnero* and shut off its SOX hotline abroad, reasoning that SOX's § 301 hotline mandate is confined to U.S. soil.

But even to the extent that strategy might be viable, SOX-regulated multinationals seem extremely reluctant to adopt it, if only because the SEC does not seem ready to accept it. Although SOX passed only in 2002, its § 301 hotline mandate has intractably taken root. In the compliance-focused environment of the new millennium, multinationals are so committed to stamping out wrongdoing via hotlines that they seem firmly committed to launching U.S.-style whistleblowing procedures everywhere they operate—even if not technically SOX-imposed.[17]

2. SOX Friction in Europe Socially

Before examining these European "foreign sovereignty…concerns" that clash with SOX § 301, we need to understand their *social context*. After all, an American might wonder, how could Europeans possibly intend to block a rule that encourages whistleblowing on corporate wrongdoing?

SOX has been widely criticized in Europe. Europeans have argued that the SOX approach of holding corporate officers to verifications of their financial statements is naive, unrealistic, expensive, ineffective, and a disincentive to being listed on U.S. exchanges. Beyond these general complaints, SOX friction in Europe regarding whistleblower hotlines specifically is rooted in two issues that permeate most SOX compliance policies: anonymous reporting, and mandatory reporting rules that force employees to denounce their fellows who commit audit/accounting frauds.

Indeed, in Northern Continental Europe (especially Germany and France), anonymous mandatory denunciations smack of WWII-era authoritarianism—neighbor spying on neighbor.[18] SOX companies' anonymous hotlines and mandatory denunciation rules have encountered intense push-back from Northern Continental European employee populations.[19] Anonymity is a special concern, because to a Northern European the cloak of anonymity lures an enemy into lodging a false

---

[14] Another argument commonly made to distinguish *Carnero* from § 301 is that *Carnero* involved a foreign-citizen plaintiff: The *Carnero* holding might have differed had the plaintiff been an American working overseas. But this distinction seems unlikely, for two reasons: (1) the vast majority of multinationals' overseas employee populations are not U.S. citizens, so the hotline and retaliation issue needs to be analyzed *as it affects non-Americans abroad*; and (2) this distinction between Americans and non-Americans working abroad appears in the texts of many U.S. *anti-discrimination* statutes, as to their application abroad. But it has no grounding at all in the text of SOX §§ 301 or 806.

[15] *Carnero*, *supra* note 13, at text accompanying decision footnote 8, and *see* decision footnote 8.

[16] *See* discussion *infra* at sections 3-6 of this article.

[17] This observation is based on the author's conversations with human resources officers and in-house employment lawyers at over a dozen multinationals, about the *Carnero* argument in the § 301 context. Because the SEC seems to assume SOX § 301 applies abroad, any multinational that invokes *Carnero* and shuts off its hotline abroad will risk litigating an SEC challenge in court, making the *Carnero* argument to a judge. As to the effect of U.S. sentencing guidelines on multinational hotlines, *see supra* note 5.

[18] Socially, this phenomenon seems most stark in former Axis power countries in Northern Continental Europe. This taboo against anonymous denunciations appears *not* to exist, to any significant degree, in Britain, Ireland or Spain, and may not be a significant issue, either, in Greece, Italy or Portugal.

[19] According to Daniel Westman, partner at the Morrison & Foerster law firm, speaking in the context of SOX employee compliance in Europe:

> It is an unfortunate historical fact that many countries—in Europe, Asia, Africa, South America—have had or still have repressive governments which use informants as a tool of repression. Apart from legalities, in some [European] countries there is a strong visceral reaction against the idea of informing' or…'denouncing' co-workers.

Attitudes Toward SOX, Whistleblowing & Hotlines: U.S. vs. Europe

	U.S.	EUROPE
Follow SOX?	Compliance critical: Important federal law	Affront to sovereignty: U.S. has no business regulating behavior in Europe
Effect of whistleblowing?	Blow whistle = expose fraud	Denounce colleague = betrayal
Whistleblower's motives?	Exposing fraud helps company and society	Collaborating with authorities by denouncing fellows curries favor for personal gain
Social policy at stake?	Stop Enron-like corporate fraud	Protect *target's* presumption of innocence and due process
Legal barriers to policy/hotline	*None*: Whistleblowing policy/hotline is management prerogative	New work rules = "mandatory subject of bargaining" (inform/consult)
Legal barriers once call placed	*None*: Data from call unregulated	Call creates data file, implicating strict rules—especially if "sensitive data" or if sent EU-to-U.S.

denunciation, out of spite. Ironically, given the conflict with U.S. SOX, Europeans' priorities here are two values most commonly associated with the *U.S.* justice system: due process and the presumption of innocence.

3. European Works Council Labor Law on "Information and Consultation" and Co-determination with Workers

Northern Continental Europeans' keen skepticism of whistleblowing "denunciations" is more than an interesting *sociological* construct. It creates *legal* ripples, via two distinct doctrines under law in Northern Continental Europe: Works council "information and consultation" (labor) law, and data privacy law. Both these doctrines can obstruct SOX-compliant whistleblower programs. Of the two doctrines, data privacy law gets more of the attention, because it is the more complex. But the completely separate works council "information and consultation" (labor) law issue is every bit as critical for multinationals trying to roll out hotlines in Europe.

In Northern Continental Europe (except Scandinavia), workers organize themselves not only into trade unions, but also into "works councils," or in-house employee representative groups with which management "informs" and "consults" (bargains) on issues affecting the workplace.[20] European employers have a duty analogous to a U.S. "mandatory subject of bargaining" to tell works council representatives about proposed changes to the workplace, and to consult with them in good faith about their opinions.[21] Launching a new rule or policy—such as a denunciation hotline—comes under this duty if the rule materially changes work conditions. Given the social taboo over denunciations, a Northern Continental European worker will see as "material" any rule that forces him to report on his fellows[22] or subjects him to a system, such as a hotline, by which his fellows can anonymously denounce him.

S. Taub, "Multinationals Find SOX is Conflicting with Local Laws," Compliance Week, July 19, 2005 (see www.complianceweek.com) (emphasis added). In one situation in early 2003 known to the author, a French employee of a U.S. multinational's Paris office sent an all-hands e-mail complaining that the company's SOX mandatory reporting rule was reminiscent of "Vichy" tactics.

[20] Works councils, which are different from European trade unions but which play a role similar to U.S. labor unions, represent employees at the company level, and have a right to offer input on terms and conditions of employment. Currently, works councils exist chiefly in Germany, France, the Netherlands, and Spain, with some also in Belgium, Austria, and Portugal. Works councils, or at least information and consultation, are coming to all EU countries via a new directive, EU Dir. 2002/14/EC (2002). These country-level works councils are entirely separate from pan-European "European Works Councils." *See generally* Donald C. Dowling, Jr., "New European Law on 'Information and Consultation' with Local 'Works Councils': Plan Now or Pay Later," 10 HR ADVISOR no. 2 p. 6 (Mar./Apr. 2004), *reprinted in* 13 INT'L HR J. no. 2 p. 5 (Spr. 2004).

[21] Essentially, in U.S. terminology, works councils in Europe have a right to be involved in issues that materially affect terms and conditions of employment. In France, specifically, there is a two-tier analysis: Works councils must be involved in change of: (1) "control of the activities of employees," and (2) "changes in internal rules."

[22] American companies abroad run into significant HR and labor union and works councils problems when they issue heavy-handed mandates purporting to force employees to report on co-workers. And in some non-European countries, such as Australia, mandatory "report-on-your-coworker" rules can be void under local employment law.

In June 2005, a German labor court invoked works council law to strike down Wal-Mart's SOX hotline.[23] Wal-Mart's policy (like most U.S. multinationals') told employees they could get fired for doing nothing—it imposed an affirmative duty to whistleblow on co-worker fraud. Also, Wal-Mart's policy (like many U.S. multinationals') went well beyond SOX by requiring denunciations of wrongdoing not only for audit and accounting fraud, but also for non-SOX violations like theft and harassment. The German labor court therefore found Wal-Mart had violated § 87 1(1) of the German Works Constitution Act by implementing its denunciation rule and hotline in Germany, via headquarters mandate, without first "co-determining" with the German works council.[24] Even though Wal-Mart is an Arkansas-based multinational that implemented a global policy at least in part mandated by a U.S. federal law, the German labor court held the global-policy context did not excuse Wal-Mart's local German subsidiary from its bargaining obligations.[25]

The *Wal-Mart* decision is procedural: It does not rule hotlines or policies *per se* illegal; it merely requires bargaining over them. And the decision breaks no new ground: German human resources has always recognized the need to "co-determine" with works councils on new policies and work rules. Indeed, Germany's *Wal-Mart* analysis also applies in other countries with tough works council laws, including France. French labor courts regularly strike down unilaterally-implemented ethics policies for failure to inform and consult.[26] For that matter, *Wal-Mart* is actually in line with well-settled *U.S.* labor law principles: Hypothetically, if the German headquarters of Daimler-Chrysler, for example, were to issue a global policy implementing some new German law—but if that global policy materially changed terms and conditions at U.S. Chrysler plants near Detroit—the company's Michigan Chrysler management, under U.S. law, could well have a duty, as a mandatory subject of bargaining, to negotiate first with the Autoworkers Union.[27]

4. French Data Privacy Law on Whistleblower Hotlines

The same Northern Continental European hostility to whistleblowing that underlies the *Wal-Mart* works councils case also explains restrictive Northern Continental European interpretations of *data protection* (privacy) laws as they reach whistleblower hotlines. All European Union states have adopted ("transposed") into their national laws the EU Data Protection Directive,[28] a privacy law that imposes rules completely unlike the data-privacy-law mandates of the U.S. The ramifications of these EU data laws are sweeping. They reach all sorts of business recordkeeping, including human resources personnel files.[29]

---

[23] *Wal-Mart, Beschluss des Arbeitsgerichts Wuppertal vom* 15.06.2005, file no. 5 BV 20/05, June 15, 2005.

[24] *Id.* The German Works Constitution Act, German BetrVG § 87 1(1), prohibits German employers from unilaterally changing "the order of the workplace and the conduct of employees" without first "informing" and "consulting" ("co-determining") with the "works council" (company-level labor representative body). In American parlance, *Wal-Mart* is a mandatory subject of bargaining case that holds Wal-Mart violated German labor law by unilaterally implementing a whistleblower system without first negotiating with worker representatives.

The penalty for violating German works council laws is that a German labor court could (as in *Wal-Mart*) strike the non-compliant policy. The works council could also (as in *Wal-Mart*) get an injunction enjoining enforcement of the policy. Ultimately, an employer that is a repeat offender could also be fined under a quasi-criminal sanction. And adverse labor law rulings in Germany can have negative public relations repercussions.

[25] *Wal-Mart, supra* note 23. Because Wal-Mart's policy made compliance mandatory—for example, it required denouncing co-worker SOX violations—it amounted to a new work rule that, under German labor law, Wal-Mart could not unilaterally implement. Incidentally, the *Wal-Mart* court mentioned along the way that Wal-Mart's policy offered employees no practical guarantee of anonymity—the *Wal-Mart* court was actually concerned that an employee using the hotline might have his call traced and his anonymity breached. In this respect, the German court's concern regarding anonymity was precisely the *opposite* of the concern in France (that whistleblower anonymity threatens denounced victims of whistleblowing), discussed *infra*. But this is not anomalous, because the German court was focusing on labor law while the French agency addressed data privacy.

[26] *See, e.g., SigmaKalon*, TGI Nanterre court, 7/15/05; *Novartis*, TGI Nanterre, 10/6/04; *Schindler Group*, TGI Versailles, 6/17/04 (all ethics policies *outside* SOX context).

[27] *Cf.* National Labor Relations Act sec. 8(d), 29 U.S.C. § 158(d). The lesson of *Wal-Mart* is that U.S.-based companies need to ensure their European subsidiaries "inform and consult" with works councils before rolling out new rules. Of course, a U.S.-based multinational's German subsidiary would be in a difficult situation if its works council refused to agree to a reasonable SOX policy—but technically, the difficulty of winning workers representatives' consent in the mandatory subject of bargaining context (and the related issue of impasse) is a venerable labor law issue with ramifications well beyond whistleblower policies.

[28] EU Dir. 95/46/EC. For a discussion by this author of the EU directive implementing ("transposition") process, see Donald C. Dowling, Jr., "From the Social Charter to the Social Action Program 1995-1997: EU Employment Law Comes Alive," 29 Cornell Int'l L.J. 43, 47-49 (1996); Donald C. Dowling, Jr., "Worker Rights in the Post-1992 EC," 11 NW J. Int'l L&Bus. I 564, 574-77 (1991).

[29] Directive, *supra* note 28. For a summary of the data directive's core provisions, *see, e.g.*, Donald C. Dowling, Jr., "Preparing to Resolve U.S.-Based Employers' Disputes Under Europe's New Data Privacy Law," 2 J. of Alt. Disp. Res. in Employment # 1 p. 31 (2000), *reprinted at* 1 Alsb Int'l Bus. L. J. 39

One specific interpretation of EU data law reaches whistleblower hotlines—and France has been the EU member state championing this interpretation. Since summer 2005, France has issued three case opinions plus three sets of regulations on the conflict between SOX hotlines and French data law.

In late May 2005, the French data protection agency, the *Commission nationale de l'informatique et des libertés* (known by the acronym "CNIL") refused to grant two SOX-regulated U.S. multinationals, McDonald's and CEAC Technologies,[30] permission to run whistleblower hotlines in France, because their proposed denunciation systems violated France's data protection law.

French data law[31] requires that companies processing personal data (about identifiable individuals) declare their data processing systems to the French data privacy administrative agency, the CNIL.[32] This is called the "*declaration* procedure." Separately, French data law also requires that data processors first get affirmative CNIL permission to process special data—including data, such as hotline reports, that could "exclude" a person from the "benefit" of a "contract," such as an employment agreement.[33] This is called the "*authorization* procedure." In other words, employers operating in France must disclose ("declare") to the CNIL all their employee data processing systems. But special systems like SOX hotlines that could affect someone's job status ("exclude" an employee from the "benefit" of an employment "contract") also presumptively need affirmative CNIL prior approval ("authorization").[34]

In *McDonald's* and *CEAC Technologies*,[35] the CNIL ruled that McDonald's and CEAC Technologies' proposed U.S.-style anonymous hotlines would threaten privacy rights of whistleblowers' denounced victims. The hotline could deprive these targets of their right to be told the denunciations against them, and of a procedure to prove their innocence.[36]

A few months after the CNIL *McDonald's* and *CEAC Technologies* rulings, on September 15, 2005, a French *court*—the *Tribunal de Grande Instance de Libourne*—decided a very similar case, the same way.[37] But this case rests on general French employment law and due process principles—not specifically on data privacy law. In *SAS BSN GlassPack*, the Libourne court ruled a former unit of Owens-Illinois violated French law when it rolled out a SOX hotline in France (GlassPack's hotline had been implemented directly as a SOX measure). The court found GlassPack's hotline "disproportionate" because it allowed anonymous whistleblowing on "fraud or theft," and thereby endangered the "individual liberties" of potential whistleblowing targets.

The *McDonald's*, *CEAC Technologies*, and *GlassPack* decisions ignited a minor international incident: SOX-regulated multinationals saw the French position as putting them in an impossible bind, and complained to French authorities and the U.S. SEC. The furor was written up in the *Wall Street Journal*, which quoted a lawyer as saying "[c]ompanies are being told 'I either have to chop off my left hand or my right hand.'"[38] The CNIL and the SEC met and discussed the conflict.

(2002) (www.wsu.edu/legal/ijrnl/dowling/). *See also* Donald C. Dowling, Jr. and Jeremy M. Mittman, "Data Privacy Laws Outside the U.S., " *chapter 15 in* Proskauer on Privacy (2006) (PLI Books, C. Wolf, ed.).

[30] *McDonald's, CNIL Délibération n°* 2005-110 (May 26, 2005); *Exide Technologies/CEAC, CNIL Délib. n°* 2005-111 (May 26, 2005).

[31] French Computer and Freedoms Law of 1978 (*loi n° 78-17 du 6 janvier 1978*), *modified by* French Data Privacy Amendments Law of 2004 (*loi n° 2004-801 du 6 août 2004*). Because France's 2004 adoption of the EU data directive was tacked onto this preexisting 1978 law, French data privacy law has some unique features that differ from data laws in other EU jurisdictions.
As to penalties for violating French data laws generally, after non-compliance following a warning, a company in France can be fined up to €150,000, and can be subject to an injunction against further violations. A subsequent violation within 5 years can be fined up to €300,000, and can also be criminal violation. Also, adverse data privacy rulings in Europe often bring serious public relations repercussions.

[32] *Id.* at art. 25.

[33] *Id.* at art. 25. This "exclude a person from entitlement to a contract" standard comes from French law, not from the EU data directive, and therefore is essentially unique to France. *Compare id.* at art. 25 *with* Directive, *supra* note 28.

[34] French data law, *supra* note 31, at art. 25. A SOX hotline, of course, could affect the job status of any employee who is the subject of a whistleblower's complaint.

[35] *See supra* note 30.

[36] SOX policies commonly retain employer control and confidentiality over internal investigations; to the CNIL, this might look little different from a secret trial where the prosecutor doubles as judge. A cultural factor in play here is that "the tradition in Europe [is for] workplace accusations [to be] conducted more like a trial." Jeremy Josephs, "Blowing the Whistle French-Style," SHRM Global Focus on-line, www.shrm.org (May 2006).

[37] SAS BSN – GlassPack, *Tribuinal de Grande Instance de Libourne* (Sept. 15, 2005).

[38] D.Reilly & S.Nassaur, "Tip Line Bind: Follow the Law in U.S. or EU",? Wall St. J., Sept. 6, 2005, at C-1 col. 1.

But neither the uproar nor the SEC's intervention moved the CNIL. Under French data law and under the French taboo against denunciations, the French cases were well-decided. But the formal discussions with the SEC did show the CNIL how its position put SOX-regulated employers in a tight bind.[39]

So on November 10, 2005, the CNIL issued guidelines offering a way out: the *Document d'orientation adopte par la Commission le 10 novembre 2005 pour la mise en oeuvre de dispositifs d'alerte professionelle*….[40] Although press reports implied that these November guidelines eliminate the conflict between SOX § 301 and French data law, in fact the guidelines adhere closely to the analysis in the CNIL's *McDonald's/CEAC Technologies* cases,[41] and make reconciling SOX hotlines with French law a tough challenge. Under these guidelines, it appears theoretically possible to set up a "confidential, anonymous" hotline in France that complies with SOX § 301 and that the CNIL would approve under its "authorization" procedure—but only if the SOX-regulated multinational is willing to set up a whistleblowing system in France radically different from "best practices" under SOX.

To get CNIL "authorization" approval under the November guidelines, an employer would have to restructure a U.S. "best practices" whistleblower hotline radically, by implementing safeguards for accused wrongdoers that are wildly inconsistent with typical U.S. practices.

The French rules:

- require limiting hotlines to accept only complaints of audit/accounting fraud and bribery (no whistleblowing on harassment, petty theft, safety violations)
- forbid requiring whistleblowing (employees who catch co-workers committing fraud retain a right to remain silent)
- forbid or severely restrict communicating that the hotline will accept anonymous calls (hotlines may in fact accept anonymous calls, but communications about hotlines and hotline operators must urge whistleblowers to self-identify)
- require notifying accused wrongdoers immediately, as soon as evidence is preserved (tipping off targets well before completing the investigation).
- require destroying files of all hotline calls that do not result in discipline or litigation.[42]

---

[39] *See supra* discussion accompanying notes 8 - 17.

[40] Unnumbered CNIL document dated Paris, Nov. 10, 2005.

[41] Cases *supra* note 29. The guidelines in theory allow the "confidential, anonymous" hotlines mandated by SOX § 301. While the guidelines severely restrict "anonymity" as understood under American-style hotline systems (discussed *infra*), they do allow anonymous calls under some circumstances (see *infra)*. Compliance with the French guidelines likely would be held sufficient for SOX § 301 purposes; to this extent, especially in light of the sovereignty issue, a U.S. court adjudicating § 301 compliance abroad (assuming § 301 extends abroad in the first place) would likely be sensitive to French sovereignty and the compulsion of foreign law.

[42] In summary, to obtain CNIL "authorization" approval under the November guidelines, a French hotline must follow 12 rules:

1. Limit reportable offenses to audit/accounting fraud; this means that the following issues, likely, cannot be the subject of the hotline—employment discrimination/harassment, ethics policy violations, antitrust issues, and possibly even bribery;
2. Eliminate any rule requiring employees who witness fraud to make a report (SOX does not technically require such a rule, but these rules are a common U.S. best practice);
3. Articulate "categories of personnel likely to be incriminated" (who will likely be the subject of such reports);
4. Keep each "whistleblower's" identity confidential, do not retaliate, and maintain the target's (alleged wrongdoer's) identity as confidential as possible;
5. Advise eligible hotline users of information, including: names of individuals who will receive complaints; scope of the hotline; that there is no mandatory obligation to report information such that you act as a whistleblower; employees have a right of access to hotline information about themselves and a way to rectify incorrect information; abuse in whistleblowing gives rise to disciplinary/legal sanctions against the individual whistleblower; no sanctions will be meted out against a whistleblower if the allegations are challenged but the whistleblower acted in good faith;
6. "Encourage" "whistleblowers" to self-identify, and communicate this "encourage[ment]" as part of the hotline description;
7. Establish a "dedicated" system for receiving complaints, with "trained" personnel communicating on a need-to-know basis;
8. In recording complaints (hotline notes), write up only necessary alleged facts, and make clear that these are merely allegations;
9. If hotline data are transferred outside of the EU (such as to U.S. headquarters or to a U.S. hotline), ensure the transmission is under an approved method (*e.g.*, safe harbor; model contractual clauses); if data go to a third party (*e.g.*, outsourced), there must be a data contract;
10. If a whistleblower's report is held unfounded, destroy the file "immediately" if "verification" is required, destroy file after 2 months, unless disciplinary or court proceedings are pending;
11. Inform the target (alleged wrongdoer) "as soon as data . . . [are] recorded" about the complaint — however, taking preemptive "protective measures" is permitted;

Additionally, hotlines based in the U.S. raise the separate problem of data transmissions outside the EU, which the EU data directive regulates under its articles 25 and 26. If hotline calls or e-mails go to U.S. headquarters or to a U.S. outsourced hotline company, consistent with EU law they must be under "safe harbor," "model contracts," or "binding corporate rules." Further, any "onward transfer" of hotline-received information from an outsourced hotline company to the employer must separately comply.

The CNIL took an unexpected step a month after issuing these November 2005 guidelines when, on December 8, 2005, it issued a completely separate set of SOX-hotline guidelines under its *declaration* procedure.[43] These December guidelines are substantively similar to the November guidelines, but procedurally they let employers launch a SOX hotline in France without awaiting cumbersome CNIL authorization. Under the December guidelines, an employer need merely report to the CNIL, on-line, that it has set up a hotline that qualifies for the December guidelines' blanket pre-authorization. Therefore, since December 2005, an employer can roll out a French SOX hotline with no prior CNIL permission at all, merely by making an on-line declaration notice to the CNIL saying it has crafted a hotline and whistleblowing policy consistent with the December guidelines.[44]

Surprisingly, while the December guidelines offer companies a simpler procedure than their November counterpart, they are not significantly more onerous. In fact, while the November guidelines impose twelve substantive mandates,[45] the December ones impose only ten.[46] Here is a summary of the differences between the November and December guidelines:

ISSUE	NOVEMBER GUIDELINES (Authorization procedure)	DECEMBER GUIDELINES (Declaration procedure)
When hotline allowed	Hotline OK only if other tools not effective under the circumstances. Hotline must complement other tools	*[not mentioned]*
Scope of hotline	Hotline must be limited in scope. A hotline with indiscriminate scope (e.g., covering breaches of corporate policies or codes of business conduct) raises serious problems. Hotlines limited in scope will receive CNIL authorization only if other CNIL-recommended rules are respected. Whistleblowing should not be compulsory for employees (no mandatory whistleblowing rule).	Whistleblowing system must be limited to: (1) financial, (2) accounting, (3) banking, and (4) anti-bribery (including SOX compliance).
Role of data controller (employer operating hotline)	Employee communications about hotline should say hotline is only for specific topics allowed. Ignore reports received on other topics, unless a report implicates company's or employees' vital interests.	Those with access to hotline calls, including outsourced service providers, must be limited, need-to-know, trained, and bound by confidentiality.
Restrictive processing of whistleblower reports	Keep whistleblower's identity confidential to ensure against retaliation. Do not tell target who denounced him. OK to accept anonymous reports, although disfavoreds. Encourage whistleblowers to identify themselves and offer data related to facts, rather than data related to persons.	Keep whistleblowers' identities confidential. Encourage whistleblowers to self-identify. Exceptions (anonymous whistleblower OK) only if: (1) Special precautions taken as to anonymous reports, and (2) organization does not encourage anonymity in whistleblowing and employee communications account for this.

12. Ensure all individuals named/identified in a "whistleblower's" report have the right to observe "his or her" data in the file (redacting others' names).

[43] CNIL, *Autorisation unique no AU-004*, Dec. 8, 2005, *Deliberation No. 2005-305 du 8 Decembre 2005 portant autorisation unique de traitements automatises…*, J.O. no. 3, Jan. 3, 2006.

[44] Obviously the burden is on the employer actually to comply with the December guidelines: A hotline and whistleblowing policy notified to the CNIL under the December guidelines but later found to be in violation violates French law.

Also, a hotline operator transmitting data abroad (say, to U.S. headquarters) or to third parties (say, a hotline operator in the U.S.) must comply with EU data law on "onward transfers" and overseas data transmissions, such as via safe harbor, model contracts, or binding corporate rules.

[45] These 12 mandates are listed *supra* at note 42. However, the December guidelines include the November guidelines as an annex, so to that extent the November guidelines remain viable, and are not in any way obsolete.

[46] To qualify for blanket-pre-approval from CNIL under the December guidelines, in summary, an employer must:

1. Limit the hotline to financial, accounting, banking, and anti-bribery whistleblowing only.
2. Get the whistleblower to identify himself, except an anonymous complaint is acceptable if (i) extra "precautions" are taken, and (ii) the employer does not publicize that complaints may be anonymous, and encourages whistleblowers to self-identify.
3. Data collected are strictly limited to necessary information.
4. Data are collected by and communicated to only the circle of those with a need to know. "External Service Providers" must comply with these restrictions.
5. Transfers of whistleblower data outside the EU must comply with the "onward transfer" restrictions of applicable data law ("safe harbor," "model contracts," "binding corporate rules").

ISSUE	NOVEMBER GUIDELINES (Authorization procedure)	DECEMBER GUIDELINES (Declaration procedure)
Employee communications	Communicate clear and extensive information to potential whistleblowers about the hotline: Who runs it; purpose/scope of hotline; its optional nature (not mandatory); employees will not be punished for not using it; who receives reports; incriminated individuals can access and rectify their data; abuse of system may result in discipline and criminal proceedings; good faith but inaccurate reports will not result in sanctions.	In addition to information that the Labor Code requires communicating, also communicate clear and complete information: Who runs hotline; objectives; sectors affected by alerts; optional nature of the system (not mandatory); no consequences for employees who do not use hotline; who receives alerts; possible personal data transfers outside of the European Union; existence of right to access and correct available for those accused; abuse of system may result in disciplinary action and criminal proceedings; good faith but inaccurate statements will not result in sanctions.
Collecting reports and facts	Whistleblower reports may be collected by any data processing means, whether electronic or not.	Facts collected must be strictly limited to areas covered by hotline. Other facts can be processed only if they affect vital interests or physical/moral integrity of employees.
Relevant, adequate and non-excessive data in reports	Hotline should only record objective data directly related to hotline scope and strictly required for verifying alleged facts.	Analysis of a whistleblower's report may rely only on objective data directly related to hotline scope and strictly required for verifying alleged facts.
Who processes reports	A compliance team should run the hotline. Limit who can see reports. Train. Require confidentiality. Communicate data collected only need-to-know. If disclosure is required outside EU, comply with data law on out-of-EU data transmissions.	Communicate reports need-to-know only. Transfers of personal data out-of-EU must be need-to-know and follow data law on out-of-EU transfers.
Deleting whistleblower report files	Immediately delete file after finding a report unsubstantiated. As to data needing verification, delete 2 mos. after case closes, unless disciplinary action or court proceedings pending.	Immediately delete or "archive" data outside hotline scope unless otherwise provided by law. Destroy or "archive" data needing verification within 2 mos. of case closing, unless disciplinary/legal proceedings pending.
Accurate information to incriminated person	Notify target as soon as possible. Allow prompt rebuttal. If indispensable protective measures are needed to preserve evidence, take immediate measures, then communicate to target.	Notify target as soon as possible. Allow prompt rebuttal. If indispensable protective measures are needed to preserve evidence, take immediate measures, then communicate to target.

The November and December guidelines, detailed as they are, nevertheless leave many questions. To answer them, on March 1, 2006 the CNIL issued yet another set of guidelines, called "frequently asked questions" [FAQs],[47] fleshing what the two sets of guidelines actually mean. The CNIL's FAQs address topics including:

- what hotlines are, under the CNIL definition (FAQ #1)
- how to "declare" a hotline to CNIL (FAQ #3)
- interplay of U.S. Sarbanes-Oxley hotlines (FAQ #4)
- how legally to make an anonymous tip (FAQ #12)
- who can use hotlines (FAQ #13)
- interplay with the duty of confidentiality under data protection law (FAQ #18)
- interplay with ethics codes (FAQ #20)

And one issue even the Frequently Asked Questions do not fully address is whether compliance with CNIL guidelines will be deemed sufficiently "proportionate" to meet the standards of the French *SAS BSN GlassPack* court case—which did *not* turn on data protection law analysis.[48]

6. Report must be destroyed immediately, or stored longer only as necessary for an active investigation.
7. Strong data security, including "passwords," is necessary for stored and transmitted data.
8. The whistleblowing system must be limited, and communicated according to set rules.
9. The target must be notified of the complaint "as soon as the data is recorded," or as soon as "protective measurers' are "implemented" to prevent the destruction of evidence.
10. The target gets access to the report, except the whistleblower's identity remains confidential.

[47] CNIL, FAQ sur les dispositifs d'alerte professionnelle, Mar. 1, 2006.

[48] See *supra* note 37 and accompanying text.

5. Opinion of the EU "Article 29 Working Party" on the EU's Probable Position Extending the French Analysis More Broadly in Europe

All European states have adopted ("transposed") a common template data law, or "directive."[49] So data privacy laws similar to France's exist across Europe. But each EU country's data law is unique. And as of mid-2006, only France had staked out a specific legal position on how its data law affects SOX hotlines. How does the SOX-§301-versus-data-law issue play out across the rest of Europe?

Americans often assume local data laws in Europe are almost exactly the same from country to country. But in practice, each EU member state's data statute differs. And each data protection bureaucracy has every bit as much power as France's CNIL to offer its own interpretations. So the European states go their own ways. Informal statements from the UK Data Protection Commissioner, for example, make clear that the UK (so far) *declines* to adopt the French interpretation: In Britain, SOX hotlines that are fundamentally fair are perfectly legal.[50]

But Britain aside, the data bureaucracies around Europe now have some EU-level guidance here—and the EU guidance is sympathetic to the French position. On February 1, 2006, the EU's "Article 29 Data Protection Working Party" (an advisory EU-level body charged with advising on EU data protection law[51]) issued an 18-page "Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the field of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime."[52] In a word, this opinion implicitly ratifies the CNIL's interpretation of data law, at least in principle. Without taking quite as hard-line a position as the CNIL, the Article 29 Working Party opinion addresses:

- "protection of the person incriminated through a whistleblowing scheme" (sec. III)
- "assessment of the compatibility of whistleblowing schemes with data protection rules" (sec. IV)
- "provision of clear and complete information about the scheme" (sec. IV(3))
- "rights of the incriminated person" (sec. IV(4))
- "security of processing operations" (sec. IV(5))
- "management of whistleblowing schemes" (sec. IV(6))
- "transfers to third countries" (sec. IV(7))
- "compliance with notification requirement" (sec. IV(8))

In essence, the Article 29 Working Party opinion recommends a slightly watered-down version of the French requirements.[53] But again, the Article 29 party's opinion is not binding—we know the U.K., for one, does not currently intend to follow it.

But other European states likely will. The EU's Article 29 Working Party is headed by a German, and Germany is widely expected to adopt his opinion, although the German bureaucratic process will be slow: Germany, uniquely, has a network of *regional* data protection bureaucracies that all need to come on board. Other Northern European countries, too, are likely to be sympathetic to the Article 29 Party's opinion—in particular, Belgium, the Netherlands, and possibly the Scandinavian countries. Southern Europe, as of mid-2006, remains a wild card. Southern European countries appear (like the U.K. and U.S.) not to harbor the strong social taboo against denouncing co-workers.

6. Theoretical "Best Practices" Strategy Options for Launching a SOX Whistleblower Hotline in Continental Europe

A SOX-regulated multinational operating in Continental Europe that takes seriously its SOX § 301-mandated duty to set up a "confidential, anonymous" whistleblower "procedure" obviously needs a strategy for complying with

---

[49] See *supra* note 28.

[50] In Britain, the Public Interest Disclosure Act 1998 is a whistleblower anti-retaliation law. The U.K. Data Protection Commissioner appears to see this law as encouraging whistleblowing, therefore requiring a narrower reading of U.K. data protection laws to accommodate it. On France's data law diverging from the EU template, see *supra* note 31.

[51] The Article 29 Working Party is an official, but merely advisory, EU body whose *raison d'etre* is advising on the EU data protection directive and how the member states should interpret it.

[52] Opinion 1/2006, 00195/06 WP 117 (Feb. 1, 2006).

[53] For analysis of Article 29 Working Party Opinion 1/2006, see "Working Party Issues Opinion on Application of EU Data Protection Rules to Internal Whistleblowing Schemes in the Context of Accounting and Financial Crime," 22 International Cooperation And Economic Integration No. 5 (May 2006)

U.S. SOX, on the one hand, and French (and Continental European) data law on the other. There is no one-size-fits-all approach, at least not available in mid-2006. Each company wrestling with this issue therefore needs to assess its European employee population distribution, its current and proposed whistleblower hotlines, and its risk-tolerance, and then work up a strategy that fits its particular operations. At least in theory there would appear to be six possible strategies, although not all of them will be viable or practical business options for major multinationals:

Strategy #1: Invoke *Carnero* and shut off the hotline in France/Europe: A theoretical legal strategy (albeit not a practical or attractive one for most SOX-compliant multinationals) would be to decide that the *Carnero* analysis under SOX § 806 should extend as well to SOX § 301. Shut off the company hotline completely in France and Continental Europe, if not elsewhere abroad—on the theory that SOX does not mandate hotlines abroad, especially where local laws discourage them.[54]

Strategy #2: Let the "tail" wag the "dog" and launch a single global hotline that complies with the French guidelines: Separate whistleblower hotlines in separate countries appear to present huge operational and philosophical problems for many multinationals. Even though all multinationals have separate vacation, holiday, overtime and other human resources policies in each country where they operate, many multinationals seem deeply committed to launching just one single global whistleblower hotline program. And this *is* theoretically possible. A company with a keen need for a single global hotline might be able to create a *French-compliant* hotline (one that guarantees callers confidentiality and accepts anonymous calls, albeit without emphasizing the anonymity feature)—and launch it *worldwide*. That hotline, of course, would fall far short of U.S "best practices," and therefore this is probably not a viable or attractive strategy for most U.S. companies. But a hotline that complies with the French guidelines should comply with SOX § 301, even if rolled out in the U.S. (the French guidelines do allow "confidential, anonymous" hotlines—albeit with the anonymity feature downplayed). Inform and consult in Europe, as necessary, on this hotline, and make any necessary data protection filings.[55]

Strategy #3: Launch a broad headquarters global policy, but do not implement it in Europe: Any company can always receive anonymous communications from anyone, including employees, about wrongdoing. Even France's CNIL cannot stop someone from anonymously contacting company leaders. As such, there might be nothing offensive—even under French law—were an American multinational *parent company* to post contact information on its general global website encouraging anyone anywhere (employee or member of the public) to submit any helpful information, anonymously or signed, to U.S. headquarters. Even if this practice *were* offensive to French or European regulators, European agencies might not feel empowered to challenge it: France's *McDonalds* and Germany's *Wal-Mart* rulings were against local French and German subsidiary companies—not American corporate parents beyond the reach of European authorities.

A multinational that decides to comply with SOX §301 with this strategy of a single, *headquarters-level* hotline would communicate its hotline procedure only on its English-language, U.S. parent website, accessible worldwide.[56] The company's foreign subsidiaries abroad would *not* ratify, translate, communicate, or "inform and consult" on that hotline locally. Rather, local entities would ignore it. To the SEC, the multinational would point to its headquarters-level globally-accessible hotline as its compliance "procedure" with SOX § 301. If the company's local foreign subsidiaries were challenged in Europe for running an illegal hotline, the subsidiaries would point out they had never ratified, endorsed, or communicated their American parent's English-language procedure.

(International Enforcement Law Reporter); Renzo Marchini, "Conflict of Laws: Anonymous Whistleblowing Hotlines under Sarbanes-Oxley and European Data Protection Laws," 1 Privacy And Data Security Law Journal 575 (May 2006).

[54] *Supra* § 1. As to why this option will not be practical or attractive for most multinationals, see *supra* note 17 and accompanying text.

[55] No U.S.-based multinational is likely ever to select this option. The existence of this option is essentially a response to the common argument that a multinational simply must have just one single SOX compliance policy and hotline worldwide.

[56] The broad global policy here would be posted on the general company website, telling everyone who might look at the website that the U.S. parent, at headquarters, will accept any SOX whistleblower complaints, anonymous or signed, from anyone, anywhere, worldwide. This broad policy would offer a postal address, e-mail address, and/or phone number by which anyone anywhere could anonymously (or over a signature) report a SOX or other violation to company headquarters in the U.S. The policy would promise that the company would investigate complaints received. SOX §301 affirmatively requires companies to establish "receipt" "procedures" like this for complaints received from anyone—not just employees. So a broad parent company global policy like this actually appears to be SOX-mandated.

However, if any European employee were ever to use a U.S. headquarters hotline, there could be data privacy law issues if U.S. headquarters transmitted headquarters hotline data back to Europe. That is, actually processing calls received from France on a U.S. hotline might raise legal problems under French law, as soon as the French employer entity got involved in remediation. Those problems would have to be addressed, case by case, if they ever actually arose.[57]

Strategy #4: Create a separate French or Continental European hotline: Retain a U.S. hotline in the U.S., but create a separate hotline for France that complies with the CNIL guidelines. And in light of the Article 29 Working Party opinion,[58] as a proactive measure it might make sense to extend that special French hotline across Continental Europe. Inform and consult with works councils in Europe, as necessary, on this "Europeanized" hotline, and make any necessary data protection filings. This option appears to be emerging as a "best practice."

Strategy #5: Launch a flexible local foreign SOX template policy to be implemented locally: A SOX-regulated multinational based in the U.S. could have its U.S. headquarters issue to local overseas (or European) subsidiaries a flexible SOX compliance *template* for the foreign subsidiaries individually to adapt to their local laws and HR conditions. This "localizable template" would be tempered to account for legal and cultural issues in Europe. For example, it might:

- offer various avenues to report ethics violations to HR or other local managers
- suggest but not mandate reporting co-workers' violations (SOX does not require mandatory reporting rules)[59]
- offer clear protections for "denounced" whistleblowing victims' rights, and grant whistleblowing victims some role in investigations
- grant stricter protections of data privacy than a U.S. policy would, pursuant to European data law
- include a suggested list of offenses about which the hotline accepts calls

U.S. headquarters could issue this foreign SOX template policy to its overseas (or European) subsidiaries, and discuss with local HR abroad how to modify it locally, taking all necessary steps (notices to local data protection authorities; "information and consultation" with works councils).[60]

Strategy #6: Have U.S. headquarters launch a global hotline for employees worldwide, communicated on the global internet, and in addition roll out appropriate local versions: A U.S.-based SOX-regulated multinational might consider combining strategies #3 and #5 by establishing *three separate* SOX compliance policies: (1) a "full-blown" U.S. policy for U.S. staff; (2) a looser version posted on the parent company global website and addressed to the world (employees and general public alike); and (3) a "Europeanized" template for local subsidiaries to adapt and ratify, consistent with local law and procedure. Simultaneously, headquarters would drive a locally-tailored employee communication initiative. Local human resources staff in Europe would inform and consult with worker representatives, as necessary, and make any necessary local data protection filings.[61]

Conclusion

Sarbanes-Oxley's requirement that listed companies set up "confidential, anonymous" whistleblower "procedures" butts into French, German, and EU doctrines of labor and data privacy law. Multinationals launching hotlines in Europe need to factor five issues into their strategy for reconciling this conflict:

(1) SOX hotline law, and its extraterritorial reach

(2) SOX friction in Europe socially

(3) European works council labor law on "information and consultation" and co-determination with workers

---

[57] A separate point: Laws in some jurisdictions—particularly in Latin America—raise potential "dual employer" concerns. In these jurisdictions, U.S. headquarters issuing global policies need to ensure headquarters cannot be argued to be a "co-employer" along with in-country local subsidiary employer entities. But because a general broad parent-company SOX policy would be open to both employees and the general public worldwide, fortunately it should not likely give rise to a viable "dual employer" argument abroad.

[58] *Supra* note 52.

[59] See *supra* notes 15-19. U.S. sentencing guidelines encourage broad hotlines ("programs") that cover all "potential or actual criminal conduct." *See supra* note 5.

[60] This "localizable template" strategy will not appeal to those multinationals convinced they need one single SOX hotline policy worldwide. But all multinationals already have various foreign local vacation, holiday, overtime, severance, and other human resources policies. Nothing in the SOX § 301 mandate requires a single global whistleblowing procedure. Many aspects of human resources policy are already local. Conceptually, reporting procedures could be, too.

[61] As to one single global hotline versus many, see *supra* note 60.

(4) French data privacy law on whistleblower hotlines

(5) opinion of the EU "Article 29 Working Party" on the EU's probable position on extending the French analysis more broadly in Europe

Factoring in these five issues, different companies will settle upon different strategies, consistent with their own particular needs, for launching hotlines that comply with both SOX and local laws. There is no one-size-fits-all approach. But there are a number of theoretical strategies, some of which are less viable or practical than others. In many cases, the best strategy for a given SOX-regulated company will likely be one of these six:

(1) Invoke *Carnero v. Boston Scientific*[62] and shut off the hotline in France/Europe, notwithstanding that the SEC does not appear to accept this approach

(2) Let the "tail" wag the "dog," and launch a single global hotline that complies with the French guidelines

(3) Launch a broad headquarters global policy, but do not implement it in Europe

(4) Create a separate French or Continental European hotline

(5) Launch a flexible local foreign SOX template policy to be implemented locally

(6) Have U.S. headquarters launch a global hotline for employees worldwide, communicated on the global internet, and in addition roll out appropriate local versions

[62] *Supra* note 13.