Companies operating internationally may face laws and regulations that, at times, appear to conflict with one another. Those companies must diligently review those laws and work to ensure compliance with all applicable legislation. One critical area where this is particularly true for U.S.-based companies operating abroad is the intersection between the United States’ Sarbanes-Oxley whistleblower law – which mandates, among a host of other things, anonymous reporting lines for employees to “blow the whistle” on inappropriate financial conduct – and other countries’ privacy and data protection laws. Those laws, and some notable judicial decisions, particularly in the European Union (“E.U.”), discourage employers from investigating employees based on anonymous complaints.

The crux of the problem is that the investigation of the employee upon whom the whistle is blown, often anonymously, will almost inevitably require the employing company to review the individual’s personnel records and other sensitive personal data. And, the handling of personal information and data is of utmost importance – particularly to individuals who are increasingly aware of the amount of personal information that is readily available about them to the rest of the world. As individuals demand greater protection of their personal information and identities, legislation aimed at protecting individuals’ privacy has exploded. While there are significant and notable differences in data protection laws among countries, this paper will focus on the somewhat uniform, and highly influential, standards of the European Union data protection rules.

In general, the United States is vastly different from the rest of the world in how it approaches the treatment of personal information.¹ This differing approach to protecting personal information is evident in the unique (and complex) interaction of other countries’ data protection laws and Sarbanes-Oxley’s requirement to maintain hotlines for corporate whistleblowing.² The globalization of the financial markets has led U.S. companies operating abroad to face an interesting dilemma in complying with Sarbanes-Oxley and not running afoul of the privacy laws intended to protect employees’ personal information that are proliferating at the same time.

² Id.
Passed in response to highly-publicized and financially disastrous corporate fraud, the Sarbanes-Oxley Act of 2002 (“SOX”) was heralded as a way to end corrupt, irresponsible corporate accounting practices. SOX was designed “to protect shareholder investment and to shore up shareholder confidence, which seriously faltered after the numerous and financially-devastating ethical lapses by publicly-traded corporations in the early years of the 21st century.”SOX had five main objectives: (1) increasing accountability of corporate executives and board members; (2) increasing the accuracy of financial information and encouraging complete disclosure; (3) improving disclosure of information by eliminating conflicts of interest both internally and externally; (4) fostering an ethical climate in which employees at all levels are encouraged to report unethical behavior to management; and (5) ensuring that those who reported would be protected from retaliation.

SOX compliance initiatives were launched by major U.S. corporations to ensure adherence to the statute’s intricate requirements. To achieve SOX’s laudable objectives, many companies enacted Codes of Conduct to guide their business operations. Those codes contain standards of acceptable and unacceptable behavior and are intended to provide decision makers at all levels of the organization with practical rules and guidance to follow and implement in their everyday business dealings. For U.S.-based companies, these codes are often developed “to inform consumers about the principles that they follow in the production of the good and services that they manufacture or sell.” Codes of conduct often cover a myriad of topics – far beyond the pure financial and accounting focus of SOX – and include topics such as harassment, employee relations, environmental issues, intellectual property, and outside employment.

Companies must work to ensure that employees, at all levels of the organization, are adhering to the standards of conduct and that the code itself is in fact setting the appropriate expectations for behavior that it was designed to. Of course, SOX requires that all companies listed on U.S. stock exchanges adopt a code of ethics for senior financial officers and persons performing similar functions. The code must include standards that promote honest and ethical conduct, including the ethical handling of any actual (or even just apparent) conflicts of interests, as well as full compliance with all applicable laws and regulations. The codes mandated by SOX must detail appropriate behavior and extensively outline the various ways in which employees can raise concerns about accounting and financial issues, or other potential violations of law.

Section 301 of SOX mandates that publicly-traded companies establish procedures for employees of the company to submit – *confidentially and anonymously* – complaints and concerns regarding accounting and auditing matters. The U.S. Congress determined that anonymous whistleblowing mechanisms – designed to encourage employees to come forward with potentially damaging information about their companies accounting

---


4 *Id.* at 399-400.

5 *Id.* at 382 (quoting U.S. Dept. of Labor, Bureau of Int’l Labor Affairs, Codes of Conduct in the U.S. Apparel Industry).
practices and internal controls – was a critical element in SOX’s attempt to prevent fraud against shareholders.

SOX, of course, also provides for employment protections for whistleblowers and prohibits companies from retaliating against employees who do raise concerns. The ability to raise concerns and question your employer’s financial position was seen as critical in the U.S. labor market where a majority of employees have “at-will” status. At-will employment means that either the employer or the employee may terminate the employment relationship at any time, for any reason. The ability of employees to voice their concerns cloaked in anonymity is, therefore, key.

While the anonymous hotlines in place at public companies across the U.S. may have been created to comply with SOX, and intended to capture concerns about accounting, internal controls and auditing matters, the hotlines are not limited to those types of issues. Routinely, indeed in many cases predominantly, the hotlines are used by employees raising concerns over general employment-related matters, such as harassment/discrimination, theft, violence, or other employee relations issues. And, those types of issues often require a review of the alleged wrongdoer’s personal information in order to investigate.

In fact, it is almost unavoidable that some personal data will be collected and analyzed when investigating a whistleblower complaint. Therefore, companies operating SOX hotlines abroad must adjust their compliance strategies and hotline procedures to ensure compliance with applicable data protection laws. Multinational companies must carefully apply their internal whistleblowing procedures to employees outside the U.S. to minimize the risk of inadvertently violating data protection rights afforded its overseas employees.

**EUROPEAN UNION DATA PROTECTION LAWS**

While SOX is almost singularly focused on protecting the whistleblower, data protection laws have a different goal. The E.U. data protection laws focus on protecting the alleged wrongdoer – the whistleblower’s target. Of course, the E.U. guidelines “make clear that these countries have no objection in principle to [whistleblowing] programs, as long as their country’s data protection requirements are respected, including that the rights of the incriminated person(s) were protected.”

The data protection laws seek to protect the due process and privacy rights of employees who are the target of any corporate investigation. “The fundamental premise of E.U. data protection legislation is that, with limited exceptions, individuals have the right to know about and control the processing of information about themselves.” E.U. protection laws allow for the personal data about E.U. residents – even in their employment capacity – to

---

be collected, processed, and used only for limited purposes and only when specific procedural safeguards have been satisfied.\(^8\)

With those data protection laws an integral part of the legal landscape, courts in both France and Germany in landmark decisions found that anonymous employee whistleblowing hotlines were unlawful – unless certain precautions and safeguards were in place.\(^9\) Those decisions “reflected the historical unease in many E.U. countries over encouraging individuals to inform against others anonymously and without an immediate opportunity for the accused person to respond.”\(^10\)

On the heels of those two highly-publicized decisions, the European Union Data Protection Working Party (“Working Party”), an independent policy arm of the European Commission, adopted a non-binding opinion related to the application of E.U. data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crimes.\(^11\) While its views are non-binding, the Opinion was heralded as “help[ing] harmonize the approach followed by national data protection authorities when reviewing specific whistleblower schemes falling within their respective jurisdictions.”\(^12\) The Opinion noted that guidance in this area was “urgently needed, especially because companies subject to the extraterritorial provisions of SOX need to be in a position to comply with specific SOX whistleblowing provisions.”\(^13\)

The Opinion provided guidance on ways to design a whistleblower program in compliance with the E.U. Data Protection Directive (the “Directive”).\(^14\) The Directive is a template set of data protection rules that E.U. member states can use to model their own data protection legislation. The Directive sets forth a number of key concepts, including the following: (i) personal data must be processed fairly and lawfully, be collected for specified, explicit and legitimate purposes, and not be used for illegitimate purposes; (ii) there should be proportionality between the data processed and the purpose for which it is collected; and (iii) procedures should be in place to ensure that inaccurate or incomplete data is erased.\(^15\) The Directive also outlines rights for the “data subject” – the individual whose personal data is being collected and handled by the “data controller.” Those rights include being informed that personal data is being collected and having the opportunity to confirm the accuracy of the collected information.\(^16\)

---

8 Id. at 3.
10 Id.
15 Id.
The Opinion also established what would – and importantly what would not – constitute an acceptable justification for implementing a whistleblowing mechanism. 17 “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 E.U. would be made legitimate.” 18 The Opinion decreed SOX as an example of a foreign law that would not provide a legitimate basis for processing personal data. 19 However, hotlines are still lawful in the E.U. because they are necessary for a legitimate purpose – the pursuit of acceptable corporate governance within the organization implementing the internal reporting mechanism.

Of course, even the pursuit of acceptable corporate governance must be achieved in a manner designed to protect the personal data of employees. A company seeking to thoroughly investigate an allegation of wrongdoing may need to review and evaluate personal data of the alleged wrongdoer(s). However, an added complication exists in the data transfer restrictions placed on personal data by E.U. member states. In general, employee-related personal data may not lawfully be transmitted from E.U. member states to the United States “unless certain compliance measures have been taken by the E.U. affiliate that is ‘exporting’ the data and the legal entity that is ‘importing’ the data.” 20 The “movement of personal data from Europe to the United States has been a focus of concern within the European Union for many years.” 21 This is due largely to a general sense that U.S. law provides inadequate safeguards for the handling of such data.

Therefore, companies seeking to transfer personal data from the E.U. to the U.S. must embrace certain procedural safeguards. Those measures must be adopted even when the data exporter and data importer are two arms of the same corporate family. Therefore, “global companies may need to institute significant adjustments to their policies, processes and systems in order to meet the minimum E.U. data protection standards.” 22 The Working Party acknowledged that transatlantic data transfers may need to occur, but expressed a strong preference for companies to collect, review and retain as much personal data as possible on a local level.

Companies are left with the task of fashioning a hotline system that will comply with the clear requirements of SOX and the data protections laws of the jurisdictions where they operate. Of course, while the E.U. Opinion and Directive provide guidance and a suggested approach, each member state may have its own interpretation of how to best handle personal data. Therefore, multinational companies must pay particular attention to any nuances of the specific member states in which they operate.

17 Id. at 2
18 Opinion Report WP117 at 3.
19 Lauer, Steven A., BNA, at 2.
21 Id. at 1.
22 Id. at 3.
**Practical Advice: Navigating the Intersection of SOX and Data Protection Laws**

Before a U.S.-based company implements an anonymous hotline for its overseas employees, it must first carefully analyze the applicable laws of the other country. Indeed, several countries require that the company first consult with involved work councils or other employees groups. This threshold step must be satisfied before any hotline can be activated.

Once a hotline has been approved, the company must determine what parameters and controls to place on the hotline. While the Working Party Opinion is viewed by many as non-binding and merely instructive, companies that operate whistleblowing hotlines in the E.U. should, at a minimum, ensure that they comply with all of the guidance on data protection offered in the Opinion (and by the particular jurisdictions in which they operate).

The company should be clear in its communications with employees and adopt detailed local policies that fully explain the scope and intent of the hotline. Companies should embrace the advice of the Working Party that the anonymous hotline ought to serve as a supplement to – and not a replacement for – other more traditional methods of dealing with internal company issues, such as employee representatives, management, internal auditors, and Human Resources.

Companies should consider the following steps to ensure that their SOX-mandated hotlines do not run afoul of E.U. data protection laws:

- Limit the number of persons entitled to report alleged improprieties or misconduct
- Limit the number of persons who may be incriminated through the hotline
- Narrow the scope of the hotlines to those subjects at the core of SOX – accounting, internal controls, and other financial issues
- Attempt to limit reporting to matters of material, financial significance
- Allow callers to raise general concerns about systems or practices without having to make allegations against specific individuals
- Provide E.U. employees with detailed disclosures regarding the scope of the hotline, including any data that may be collected and any rights that they may have in reviewing/challenging that data
- Remind E.U. employees of other mechanisms to raise concerns, such as Human Resources staff or office management
- Encourage employees to identify themselves, but do not prohibit the submission of anonymous complaints
- Inform potential whistleblowers that they will not suffer adverse actions for raising the concern and that the matter will be investigated as confidentially as possible
- Inform alleged wrongdoers as soon as possible after a complaint has been lodged against them, unless doing so would hamper the investigation
- Inform employees that individuals abusing the reporting system or making allegations without a good faith basis may be disciplined
- No retaliation for good faith use of the hotline
In addition to these basic hotline scope and structure issues, the company must adhere to all regulations governing the transfer of any personal data collected in response to hotline complaints. Therefore, in order to comply with E.U. law, the following procedures should be adopted:

- Limit the types and amount of personal data collected (i.e., use only the data that is necessary to verify and investigate the precise allegations made)
- Attempt to handle complaints locally, if possible, to avoid any international transfer of personal data
- If international data transfer is necessary, be sure to comply with all data transfer requirements
- Only transfer data when the recipient has agreed to provide adequate safeguards
- Retain the personal data only as long as necessary and destroy/delete within a few months of completion of the investigation

The list above is not exhaustive, but hopefully provides some helpful, practical tips to enable companies to implement a meaningful mechanism for employees to blow the whistle on financial improprieties without sacrificing the privacy rights of employees.

**CONCLUSION**

Transatlantic compliance with both SOX and E.U. data protection law is possible, but requires familiarity with both SOX and the particular data protection stance of the E.U. member state in which a company operates.

Throughout 2006, the U.S. Securities and Exchange Commission and the Working Party exchanged correspondence in an effort to clarify the intersection between SOX and E.U. data protection laws. As commentators have noted, “with carefully crafted E.U. whistleblower policies and procedures, U.S. companies can now strike a balance between E.U. data protection laws and SOX, and substantially if not fully comply with both regimes.”

Multinational companies will need to periodically review legal developments in the U.S. and E.U. and their compliance programs to ensure that they have not fallen out of compliance.

Finally, while this article focused on the relatively well-known personal privacy and data protection laws of the E.U., it must be noted that data privacy laws are proliferating around the globe. U.S. companies striving to comply with SOX’s laudable goals must constantly review the legal landscape in the foreign jurisdictions in which they operate to ensure that their efforts to promote corporate accountability and transparency do not come at the cost of their employees’ right to privacy.

---

Tanya Axenson Macallair has been in-house counsel at Constellation Energy Group in Baltimore, Maryland since the Fall of 2007. Ms. Macallair serves as Senior Counsel for Human Resources and is a member of the Company’s Corporate Compliance team. She provides advice and counsel on the full spectrum of labor and employment laws and regulations for Constellation’s domestic and international operations. Ms. Macallair also assists in Constellation’s Corporate Compliance initiatives, including maintaining its Principles of Business Integrity code and overseeing its employee complaint mechanisms.

Prior to joining Constellation, Ms. Macallair was an associate in the Washington, DC office of Gibson, Dunn & Crutcher LLP. Ms. Macallair was a member of the firm’s Labor & Employment Law and Litigation Groups.

Ms. Macallair received her law degree from the Harvard Law School and her undergraduate degree from the School of Industrial & Labor Relations at Cornell University.

Constellation Energy Group is...

- A leading supplier of energy products and services to wholesale and retail electric and natural gas customers.
- A major generator of electricity with a diversified fleet of generating units strategically located throughout the United States and Canada, totaling approximately 7,100 megawatts of generating capacity.
- Among the leaders pursuing the development of new nuclear plants in the United States.
- A regulated distributor of electricity and natural gas in Central Maryland through our utility, Baltimore Gas and Electric Company.