The HSBC firms took a number of remedial actions, including contacting the customers affected, improving staff training, and requiring that all electronic data in transit be encrypted. Further, due to the firm's cooperation, their fines were discounted by thirty percent, which is reflected in the amounts discussed above.

Sanctions

OFAC Imposes $9.4 Million Fine against DHL for Sanctions Violations

U.S. Treasury Department, Press Release TG-259 (August 6, 2009)

On August 6, 2009, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) and the U.S. Department of Commerce's Bureau of Industry and Security (BIS) announced a $9.4 million settlement with DPWN Holdings (USA) Inc., formerly known as DHL Holdings (USA) Inc. and DHL Express (USA) Inc. (collectively DHL) as a result of shipments to Iran, Sudan and Syria and recordkeeping violations.

DHL allegedly violated the following OFAC regulations: the Iranian Transactions Regulations (ITR); the Sudanese Sanctions Regulations (SSR); and the Reporting, Procedures and Penalties Regulations (RPPR). Under these OFAC regulations, shipments of most goods to Iran and Sudan are prohibited, and require the maintenance of complete records on shipments for five years. The company allegedly also violated the Department of Commerce's Export Administration Regulations (EAR). *See* Treasury's Press Release TG-259 (August 6, 2009).

According to OFAC, DHL made more than three hundred shipments to Iran and Sudan between August 2002 and March 2007 in violation of the ITR and SSR, and failed to keep records of other shipments to Iran between December 2002 and April 2006 in violation of the RPPR. As mentioned in the Press Release, thousands of airway bills did not contain descriptions of the contents of the packages.

The $9.4 million settlement was the culmination of a five and a half year investigation that OFAC conducted with the assistance of the U.S. Department of Homeland Security's Customs and Border Protection, which intercepted many of the shipments and reported them to OFAC.

In addition to agreeing to pay the $9.4 million fine, DHL agreed to make major improvements in its compliance program with regards to OFAC Regulations and the EAR, including hiring an independent third-party consultant to conduct audits of its compliance covering the period from March 2007 through to 2011.

As OFAC Director, Adam J. Szubin, indicated in the Press Release, the enforcement action against DHL was a signal that the government is committed to ensuring compliance with sanctions laws.

Internal Investigations & Oversight

Corporate Communications

U.S. Internal Investigations and Foreign Data Protection Laws

Contributed by: Philip Urofsky and Grace Harbour of Shearman & Sterling LLP

Introduction: Balancing European Data Privacy Concerns with the Need for Information in an Internal Investigation

With the globalization of laws focusing on corruption, money laundering, and financial fraud, professionals working in compliance are facing new challenges. Across Europe, "data protection" or "data privacy" policies at both the European and national levels restrict companies' ability to collect, process, review, or transfer data containing various kinds of personal information. Although not intended to shield malfeasant employees, these data privacy policies may pose obstacles to internal compliance procedures that rely heavily on documentary information to identify and investigate areas of potential misconduct and to monitor compliance efforts. This article examines the challenges that compliance professionals and external counsel face in attempting to comply with European data privacy laws while effectively enforcing internal compliance policies and procedures and domestic and international anti-corruption, money laundering, and financial fraud laws, including the United States' Foreign Corrupt Practices Act (FCPA).[1] This article identifies the tensions between internal compliance investigations and European data privacy regimes and offers solutions that serve both interests when possible and compromise when necessary.

Information Gathering in an Internal Investigation

Goals of an Investigation

U.S.-based and multinational companies often hire private counsel to investigate potential internal misconduct. This could be in conjunction with a government investigation, in anticipation of government action, or as a matter of routine compliance. Such internal investigations are intended

to uncover any potential wrongdoing and to ensure that problem areas are addressed to avoid repetition. Further, a thorough investigation enables a company to make informed decisions about risks relating to personnel, projects, agents, consultants, vendors, and customers; decide whether to voluntarily disclose an investigation's findings to a government regulatory or enforcement agency; and devise an appropriate strategy to respond to potential government investigations or other types of litigation.

Cooperation with the Government Regulatory and Enforcement Agencies

It is not appropriate in every case in which a potential violation is discovered to make a voluntary disclosure to the government. In some cases, the issues identified through an internal investigation may be dealt with internally or, indeed, an investigation may conclude that the allegations under investigation are unfounded. In other cases—especially where the allegations appear to have substance or involve serious issues, and the government knows or is likely to find out about them—the company may decide to disclose the results of its investigation to the government, pledge its cooperation, and seek time and forbearance from the government to complete its internal investigation.

In the United States and increasingly in foreign jurisdictions, governments may agree to stand aside for a reasonable period to allow a corporation to investigate itself. Long a standard practice in the United States, government regulatory and enforcement agencies outside the United States, and the companies subject to their jurisdiction, are increasingly embracing private internal investigations as an efficient and expedited alternative to a government investigation, albeit with varying degrees of government supervision and monitoring. The benefit of an internal investigation is that it spares companies from an overly protracted, intrusive, and unpredictable government investigation. However, a government agency's willingness to permit a private internal investigation and to accept its findings without conducting its own follow-on investigation will necessarily depend on the credibility of the investigation, including the company's ability to provide assurances of thorough data preservation, collection, and review.

In the United States, independent internal investigations often help the U.S. authorities to decide whether to take enforcement action under the FCPA, the False Claims Act, the securities acts, and other statutes. The more thorough and balanced an investigation, the more likely the authorities are to determine that government intervention is unnecessary or to be lenient with any potential fine or judgment. Making visible efforts to cooperate with the United States government could go a long way toward deterring criminal or civil prosecutions and other enforcement actions.[2] Such cooperation includes timely and voluntary disclosure of facts relevant to potential wrongdoing. The government will look more favorably on companies that are willing to identify relevant actors and provide relevant information, including documentary evidence. On the other hand, actions that tend to obstruct an investigation, including delayed or incomplete production of requested documents, will weigh against a company. Thus, data privacy laws may create potential obstacles by limiting the scope of information that can be reviewed or produced to the authorities in the United States. This could have a negative impact on the investigation's credibility, the authorities' willingness to permit an internal investigation, and, of course, the authorities' ultimate enforcement determination.

Some U.S. prosecutors, particularly those in the headquarters units of the Department of Justice (DOJ) and the Securities and Exchange Commission (SEC), have a sophisticated understanding of European data issues and endeavor to distinguish between companies that face *bona fide* difficulties in obtaining, reviewing, and eventually producing European data and those that raise strategic and unreasonable claims of data protection difficulties to create unnecessary obstacles to production of relevant information. In the former case, U.S. enforcement officials are likely to work cooperatively with the company to obtain the information through established government-to-government channels. In the latter case, the authorities may independently seek foreign law enforcement cooperation that could potentially trigger foreign investigations, cause foreign employees to be interviewed by their local police, and lead to compelled production of data of a broader scope than would have resulted from a more cooperative stance.

European Data Privacy Regimes

The European Union's Data Privacy Directive

The European Union's Data Protection Directive 95/46/EC (Directive) is the primary legislation on data protection in Europe.[3] The purpose of the Directive is to foster free movement of personal data among European Union (EU) member states while safeguarding European citizens' fundamental right to privacy. By establishing a uniform level of data protection across all member states, the Directive aims to eliminate barriers to information flow that might arise from differing standards of protection of privacy rights. The Directive requires EU member states to pass domestic laws implementing the Directive's data privacy protections.[4] In addition to EU member states, European states that are not members of the EU such as European Free Trade Association (EFTA) states,[5] Russia,[6] and Switzerland[7] have also passed data privacy legislation offering protections comparable to

those in the Directive. Some non-European states have also followed Europe's lead in enacting data privacy laws.[8]

Data Privacy under the Directive

The Directive places restrictions on the type of data that may be processed and the circumstances in which processing is permissible. The Directive also limits what can be done with European data outside of the European Union in jurisdictions—such as the United States—that in the eyes of the European Union do not have comparable data privacy protections.

Protected Data

The Directive protects "personal data," which is defined as "any information relating to an identified or identifiable natural person."[9] The Directive's broad definition of personal data includes not only data ordinarily considered personal, but also business data that refer to employees, customers or clients, or other parties by an identifying characteristic. This would include, for example, employee phone numbers, human resources records, and medical information.

Parameters of Permissible Data Processing

The Directive defines data "processing" broadly to include "any operation…which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction" of data.[10]

The Directive permits data processing only in limited circumstances. If the data subject has unambiguously consented to having his or her personal data processed, data processing is permissible.[11] This raises questions about the parameters of consent, addressed in more detail below. The Directive also allows data to be processed when necessary to perform on a contract, to comply with a legal obligation, or to perform a task in the public interest.[12] Finally, data processing is permissible "for the purposes of the legitimate interests pursued by the…parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject."[13] An internal investigation into potential illegal activity by a company's employees or agents may seem to fit into at least one of these categories where processing is permissible, but the domestic regulatory authorities do not always agree, as discussed further below.

Restrictions for Nations with Inadequate Data Privacy Protections

Under the Directive, personal data may not be transferred to countries that do not have similar levels of data privacy protection.[14] The European Commission decides whether or not a country qualifies to receive data transferred from Europe.[15] Countries deemed to be without comparable data privacy policies may take measures to ensure adequate data protection, which would then allow them to receive data transferred from European countries. These measures could take the form of domestic laws or other international commitments, and their adequacy is determined by the European Commission.[16]

The United States is not among the countries that the European Commission has deemed to have adequate data privacy laws.[17] However, the U.S. Department of Commerce and the European Commission negotiated a "safe harbor" exception that allows American companies who voluntarily adhere to certain data protection principles to transfer data from the European Union to the United States.[18] Law firms, accounting firms, and document processing vendors who are safe harbor compliant are permitted to process personal data.

Another way to facilitate data processing from Europe is to enter into a data protection contract. The European Commission has approved two model contractual clauses that would satisfy the Directive's data privacy restrictions. These contractual clauses must be adopted verbatim.[19] Agreements containing these approved data privacy clauses are between a data exporter in an EU or EFTA country and a data importer in a non-Directive approved country. In the context of an internal investigation, the data exporter would be the client and the data importer would generally be the law firm receiving the data. The data importer is responsible for ensuring that intermediate vendors that receive the data, such as data processors and database hosts, comply with the data privacy agreement.

Domestic Enforcement

As challenging as it may seem to balance the Directive's data privacy policies with a comprehensive internal investigation, the real difficulty arises from domestic enforcement in EU and EFTA member states. The Directive sets forth minimum data privacy standards that domestic legislation must meet, but often domestic data privacy laws are more restrictive than the Directive. In Germany, for instance, an individual's consent to allow his or her data to be processed is only effective if it is "freely given," and there is some debate over whether consent given at the request of an employer during an investigation meets this requirement.[20] Meeting the consent requirement may take time and significantly delay an investigation. For various reasons, the most obvious being potential culpability, employees may refuse to consent to the processing and review of their documents and it can be a time-consuming and costly process to negotiate the terms of their consent.

Dealing with domestic data protection authorities can be difficult and unpredictable. In some countries, parties must obtain permission from the regulatory authorities before processing data, which can be a slow process.[21] Regulatory authorities vary in their interpretations of data privacy provisions, with some reading the provisions more strictly than a natural reading might suggest. For example, during one international anti-corruption investigation, the staff of one European country's data privacy commission sent a letter to the company indicating that reviewing emails was categorically prohibited by the Directive and the domestic privacy law unless each and every person named in each email gave consent in advance. In this instance, the company disputed the staff's interpretation and the commission itself did not pronounce on the issue. Ultimately, the company proceeded with the data processing and review as planned, but only after a significant delay. This example is just one of many that illustrate the unpredictability that compliance professionals might face from regulatory authorities.

Works Councils and Other Workers' Rights Issues

In addition to government-instituted data privacy regimes, dealing with European works councils and other workers' rights systems may also pose significant challenges to an internal investigation. Works councils are organizations that inform and consult employees about company-wide issues that implicate local employees and represent their constituents' rights and interests. Many European nations have domestic laws that require companies to have works councils to protect the interests of employees. Depending on its mandate, a works council could be very involved in the investigation process, particularly where data privacy issues are concerned. For example, a works council may act as an intermediary between an investigation team and the employees, requiring document preservation notices, collection notices, and interview notices to be negotiated with and approved by the works council. Works councils may also play a role in enforcing data privacy policies. Thus, in addition to obtaining the consent of individuals before an individual's data may be processed or reviewed, it may be necessary to obtain the consent of a works council. In a recent investigation, a company's works council took the position that certain data relevant to the investigation included personal information and threatened to seek a court order prohibiting the company from processing and reviewing such data. The resulting costly delays endangered the investigation by raising unnecessary suspicions that could have provoked intervention from the government investigators, whose ability to obtain such data is subject to fewer restrictions under the Directive than are private parties.

Although works councils are often mandated by law, the scope of their role in protecting employees' data privacy interests is sometimes determined by custom or common practice. This applies equally to other workers' rights systems concerning data privacy that, although not defined by law, allude to certain rights to which employees assume entitlement. Whether driven by works councils or another source, such de facto workers' privacy rights can complicate and delay an internal investigation. For example, a recent internal investigation ran into difficulty collecting data from employees' company computers because the company had told its employees they could use their work computers as if they were personal computers, thereby giving rise to an assumption of privacy rights with respect to data on the company computers.

Blocking Statutes

Although they do not directly implicate data privacy, blocking statutes can also restrict access to information in a U.S.-based internal investigation. A number of countries have enacted blocking laws that prohibit cooperation with U.S. discovery demands meeting certain criteria. These statutes impose criminal or civil sanctions on those who comply with discovery requests directly, bypassing the much more cumbersome channels set forth in the Hague Evidence Convention. This effectively requires companies and individuals who receive such requests to balance potentially violating a foreign blocking statute against the risk of being compelled to produce the data by a U.S. court. In the context of an internal investigation, a company may be concerned that by transporting data to the United States for review by its counsel, that data could potentially be subject to subpoena in a U.S. civil or criminal matter. Once such data is subpoenaed, courts in the United States may compel compliance with discovery even if a blocking statute in the data's source country would impose sanctions.[22] Depending on how the company, on the advice of its counsel, evaluates this risk, it may agree to produce data for review only within the data's source country.

Practical Pointers on Dealing with Data Privacy Concerns in an Internal Investigation

Preliminary Measures

Understanding the contours of a given country's implementing legislation and how its regulatory body approaches data privacy policies will allow compliance professionals to devise an informed plan for information gathering that maximizes the investigation's efficacy while avoiding data privacy conflicts. Given the complexity and variance of data privacy regimes across Europe, an important first step in dealing with data privacy concerns in an investigation is to consult with local counsel with data privacy experience to advise on these issues. In some cases, particularly for multinational corporations, the company may have such expertise in-house. In other cases, it will be necessary to retain local external counsel. In addition, the company's local human resources and legal staff should

be consulted for information on how data privacy issues have been addressed in the past within the company, including the role of works councils and data-sharing between the parent corporation and its subsidiaries and affiliates.

Data Collection

Data privacy concerns begin with document preservation notices sent to employees instructing them to retain and refrain from altering documents that could be relevant to the investigation. Preserving data at the outset of an investigation is important because potential resistance from regulatory authorities and employees refusing to give consent may significantly delay document collection, processing, and review. The preservation process begins with a general retention notice to employees, after which the company's technology department or an outside vendor segregates the relevant data to ensure that it is not deleted. Preservation secures data pending resolution of these potential issues.

Preservation notices are followed by document collection notices to specific employees notifying them that their documents are going to be collected, identifying a collection time, and setting out the manner of collection. It may be necessary to consult with your client's human resources professionals or labor lawyers concerning the potential role of works councils in the preservation and collection notices to preempt later objections.

Prior to the actual collection, counsel or the forensic data collector should meet with each employee individually to go over the process and to answer any questions. This collection interview should be carefully memorialized. The focus of the interview should be on specific issues related to the data collection and not on the facts or conduct under investigation.

These collection interviews serve several purposes. First, they allow the employee an opportunity to identify potentially personal data, thus enabling the company to take the necessary steps to minimize the personal information retrieved while maximizing information relevant to the investigation. To the extent possible, personal or private data should be segregated from the start. Thus, during the collection interview, employees should be asked to identify any folders dedicated to personal information. Second, collection interviews may also help generate search terms to identify documents that are likely to be private or personal. Third, the collection interview provides valuable information concerning the location and organization of the employee's hard copy and electronic files, the identity of persons with access to such files, whether the employee uses other computers (both company and private), whether the employee saves data onto external media (such as disks, memory sticks, internet storage locations), and whether the employee maintains any files (hard copy or electronic) at home.

Although consent is arguably not necessary in all circumstances, it is generally prudent to obtain a signed consent from every person whose data is to be collected and, in some circumstances, from works councils. The form and effectiveness of a written consent is dependent on local law. If possible, companies should try to obtain employees' consent to waive data privacy protections at the start of employment. The challenge to an advance waiver is that it must be narrow enough to meet consent specificity requirements set forth in data privacy legislation but not so narrow as to exclude information that could become relevant in a future investigation.

If the custodian is not willing to consent, the company must weigh its options. Depending on local law, the company may take the position that data and documents located on company computers and stored in company facilities are property of the company, including private material. The company could then process the data without consent. Such a position may well be justified under local law, but a company that proceeds in this fashion should obviously consult with local counsel with expertise in this area. In some cases, the company itself may be permitted to review the files but not outsiders. In such a case, the company may have auditors or in-house counsel review the data and then provide outside counsel with "anonymized" relevant data to allow counsel to provide it with legal advice. In other cases, the company may have the right to take employment action against uncooperative employees (although this may not be available if the employee is within his or her rights in refusing consent).

Data Processing

Before entering the data processing stage in an internal investigation, compliance professionals should consider how to comply with the Directive's restrictions on data processing. Investigations in countries with strict data privacy regimes may consider processing all data within that country and exporting only clearly relevant, non-private data to the United States or elsewhere. Doing so, however, may add to the time and cost of processing because processing data in different locations eliminates the possibility of using software tools such as "de-duping," which consolidates duplicative data (such as identical documents found on different computers or the sender's and recipients' copies of the same email).

If, for the sake of convenience or to minimize costs, the company chooses (or authorizes its counsel) to process the data in the United States, it must either use a data processing vendor that is self-certified as safe harbor compliant[23] or enter into one of the model data protection agreements approved by the European Commission. If the latter is chosen, the company or the law firm responsible for exporting the data to the United States must ensure that every intermediate data

processing vendor given access to the data complies with the data privacy agreement. In addition to ensuring compliance with the Directive, confidentiality agreements should be executed with all vendors who will have access to the data. As an extra security measure, documents that contain the names of custodians or other information protected by the data privacy laws may be encrypted in preparation for transfer.

Under the Directive, data is "processed" almost from the beginning of the process when it is copied. As a practical matter, the processing may take place in several stages: copying, loading into a database, running search terms, and reviewing specific data. The ultimate purpose of these stages is to arrive at a manageable set of potentially relevant data that can then be reviewed to identify documents with actual relevance. This requires careful balancing to ensure that the data set is not unduly extensive (and thus prohibitively expensive to review) but not unduly narrow (and thus missing relevant data).

Data Review

After documents have been processed, an investigation team may consider allowing employees to review the collected documents first and identify documents that they deem personal. This may take place either before or after search terms have been run. Doing this earlier has the advantage that private data never enters the database but doing it later reduces the volume that needs to be reviewed by the employee. This kind of preliminary employee review will slow down the investigation but may be a useful compromise for compliance professionals facing resistance from a works council or data protection authority.

There is a risk, of course, that an employee, out of a variety of motives, may mark as personal or private certain data that is neither and that is, moreover, relevant to the investigation. Accordingly, the investigators should create a mechanism through which the potentially personal documents are reviewed, while at the same time segregated from the general population of data. The purpose of reviewing potentially personal documents is to verify that they are indeed personal or private, so review could be limited to a single compliance attorney or in-house counsel.

Data Production

An internal investigation may run into data privacy roadblocks when the time comes to produce data to a government agency, particularly one outside the country in which the data was collected. Clearly, the more narrow and specific the disclosure is, and the more the data is obviously relevant to potential wrongdoing, the less likely it is to result in a successful data protection challenge. Further, it may be possible to produce redacted data that does not divulge information protected by the data privacy laws. In some cases where the relevant government agency is unlikely to pursue individuals, *e.g.*, for lack of jurisdiction or due to parallel government investigations, it may even be possible to "anonymize" the data, thus allowing the government agency to focus on the acts of the corporation rather than specific individuals.

In addition or as an alternative, parties may negotiate a confidentiality agreement or seek a protective order such that all documents produced in the course of an investigation would be considered confidential and protected against disclosure to unrelated third parties. Even if the government authorities were to agree to such an agreement or order, however, it would necessarily contain exceptions to allow for any disclosure that might be required during discovery in a criminal or civil enforcement action. The agreement or order, therefore, should include provisions obligating the U.S. enforcement authorities to obtain a similar agreement or order applicable to any parties to whom it is required to disclose the data. Furthermore, of course, if the government went to trial against the company or any other parties, either side may well need to use the data as evidence and it would be difficult to maintain its confidentiality at that point.

Finally, and this is obviously the least preferable but sometimes the only alternative, the company can provide guidance to a government agency to allow it to make an official request for cooperation to its counterpart in the country in which the data is located. If the foreign agency was not previously aware of the internal investigation, or is not inclined to condone internal investigations, such a request may complicate the company's efforts to proceed efficiently and expeditiously toward an ultimate resolution. Further, it obviously opens up an avenue by which the governments may go down unforeseen and unproductive paths, thereby increasing the cost and duration of the investigation. On the other hand, by encouraging cooperation and communication between the two government agencies, the company may be able to avoid duplication and second-guessing and ensure that both governments ultimately accept the investigation's findings.

Conclusion

The first step toward balancing employee data privacy concerns with the need for information in an internal investigation is being aware of the potential conflicts between the two. Every investigation taking place in Europe should begin with input from local counsel and local personnel who are de facto experts on a given country's data privacy regime. Anti-corruption investigations require thorough research, creative planning, and flexibility to deal with unexpected hurdles that might come from regulatory bodies or works councils. Compliance professionals must be informed and creative to successfully and comprehensively gather the information

necessary to cooperate with the government agencies while complying with domestic data privacy laws.

Philip Urofsky is a litigation partner at Shearman & Sterling LLP, specializing in internal investigations and white collar corporate and individual defense, including in FCPA, economic sanctions, and money laundering matters. Prior to joining Shearman, he was Assistant Chief of the DOJ's Fraud Section, where he supervised or handled FCPA investigations and prosecutions, assisted in negotiating international anti-corruption treaties and follow-up peer reviews, and drafted the first Principles of Federal Prosecution of Corporations (the "Holder Memo"). He can be reached at philip.urofsky@shearman.com or 202/508-8060. Grace Harbour is a former litigation associate at Shearman & Sterling LLP. Beginning in August 2009, she will be at the Office of the Prosecutor at the International Criminal Tribunal for the former Yugoslavia at the Hague. She can be reached at graceharbour@gmail.com.

[1] 15 U.S.C. § 78dd-1, *et seq.*
[2] *See* Principles of Federal Prosecution of Business Organizations, (DOJ website last visited June 11, 2009).
[3] Directive 95/46/EC of the European Parliament and of the Council of 24 (October 1995) on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter "Directive").
[4] *See* Justice and Home Affairs – Data Protection – The Law – Status of Implementation of Directive 95, (last visited June 11, 2009).
[5] *See id.*
[6] Russian Federation Law on Personal Data, Law 152-FZ (July 27, 2006); *see generally* Privacy International PHR2006 – Russian Federation, (from the Privacy International home page, follow the "Country Archives" link on the left-hand menu, click on "Russia", and select the link labeled "PHR 2006 – Russian Federation") (last visited June 21, 2009).
[7] Swiss Federal Data Protection Act of 1992, DSG, SR 235.1 (June 19, 1992); see generally Privacy International PHR2006 – Swiss Confederation (Switzerland), (from the Privacy International home page, follow the "Country Archives" link on the left-hand menu, click on "Switzerland", and select the link labeled "PHR 2006 – Swiss Confederation (Switzerland)") (last visited June 21, 2009).
[8] See, e.g., Argentine Law for the Protection of Personal Data, Law No. 25.326 (November 2, 2000), amended by Law No. 26.343 (January 9, 2008); see generally Privacy International PHR2006 – Argentina, (from the Privacy International home page, follow the "Country Archives" link on the left-hand menu, click on "Argentina", and select the link labeled "PHR 2006 – Argentina") (last visited June 21, 2009); Israeli Protection of Privacy Law 5741-1981, 1011 Laws of the State of Israel 128, amended by Law 5745-1985; see generally Privacy International PHR2006 – State of Israel (from the Privacy International home page, follow the "Country Archives" link on the left-hand menu, click on "Israel", and select the link labeled "PHR 2006 – State of Israel") (last visited June 21, 2009).
[9] Directive, Article 2(a).
[10] Directive, Article 2(b).
[11] Directive, Article 7(a).
[12] Directive, Article 7(b)-(d).
[13] Directive, Article 7(f).
[14] Directive, Article 25.
[15] Directive, Article 25(4); see EU's Justice and Home Affairs – Data Protection – Adequacy of the Protection of Personal Data in Third Countries, (website last visited June 11, 2009).
[16] Directive, Article 25(5)-(6).
[17] *See* EU's Justice and Home Affairs – Data Protection – Adequacy of the Protection of Personal Data in Third Countries (website last visited June 11, 2009).
[18] Fed. Reg. 45666-01 (July 24, 2000).
[19] Directive, Article 26(4); model contracts available on the EU's Justice and Home Affairs website (last visited June 11, 2009).
[20] See German Federal Data Protection Act § 4(a).
[21] See, e.g., German Federal Data Protection Act § 4(d) (requiring registration of data processing procedures) (last visited June 11, 2009); Spanish Law on the Protection of Personal Data Article 33(1), available on on the EU's Justice and Home Affairs website (under "Spain," click PDF icon labeled "Unofficial English Translation") (requiring authorization to be obtained from the Director of the Data protection Agency before data may be transferred to non-Directive countries).
[22] Cf. *In re Grand Jury Subpoenas Dated March 19, 2002 and August 2, 2002 (The Mercator Corp., James H. Giffen, and Akin, Gump, Strauss, Hauer & Feld, LLP v. U.S.)*, 378 F.3d 379 (2nd Cir. 2003) (enforcing grand jury subpoenas for Swiss bank records brought to the United States for review by a law firm).
[23] A list of safe harbor compliant companies can be found on the United States Department of Commerce website.

Corporate Counsel

Reducing the High Price of Internal Investigations: Five Cost-Saving Suggestions for Conducting a Cost-Effective Investigation

Contributed by Paul J. McNulty, Joan E. Meyer, and Brian L. Whisler, Baker & McKenzie

Corporate internal investigations are expensive – often very expensive. Determining the "who did what when" of business misconduct usually requires document review, forensic audits, employee interviews, legal research and report preparation. These are time-consuming and resource-intensive tasks. Depending on the scope and seriousness of the matter, investigations can stretch out over many months and, in some cases, even years.

Foregoing an internal investigation altogether is generally not an option. Corporate directors and senior managers have a fiduciary duty to investigate credible allegations of misconduct. And the most expensive investigations are often the ones that need to be voluntarily disclosed to the government in an effort to reduce or avoid heavy penalties. Companies simply need to know what happened, and a "see no evil" strategy will not work.

The challenge, therefore, is to conduct a credible internal investigation in a cost-effective manner. "Credible" means an investigation that the government would view as sufficiently thorough and independent. Why independent? A primary goal in any investigation should be to develop a factual record that prosecutors would accept as a reliable basis for moving forward with discussions of a resolution (should that be necessary), rather than launching their own separate investigation. That outcome, by the way, is no small accomplishment. It could spare a company the tremendous burden of responding to subpoenas, search warrants and prosecutor interviews. This, of course, is why most significant internal investigations are conducted by law firms rather than in-house counsel. Whether true or not, the government perceives lawyers outside of the corporate structure to be in the best position to make an independent assessment of whether a violation has occurred.

A growing number of corporate general counsel suggest that a cost-effective outside investigation is an oxymoron. Stories of exorbitant attorneys' fees for internal investigations are a hot topic at in-house counsel gatherings. And because many