Bloomberg BNA

Privacy and Security Law Report®

Preventing Corruption While Protecting Personal Information



BY SUHNA PIERCE, MARIAN WALDMANN AGARWAL, AND RUTI SMITHLINE

Multinational businesses are subject to a patchwork of laws of the various jurisdictions in which they operate. Complying with the myriad rules and regulations can be challenging. Compliance obligations vary from one country to another, even where countries within a market (such as the European Union) have a deliberately harmonized approach. To add to the complexity, requirements under one jurisdiction's laws sometimes create tension with another's. For example, more and more companies are implementing due diligence processes for engaging third parties in order to reduce the risks of violating anti-corruption laws, such as the U.S. Foreign Corrupt Practices Act[1] (FCPA) and the U.K. Bribery Act 2010[2] (''U.K. Bribery Act''). However, their due diligence programs may unwittingly expose them to risks under privacy and data protection laws around the world.

More than 70 countries currently have a privacy or data protection law. These laws regulate the collection and use of personal information, which generally means any information pertaining to identified or identifiable individuals. Because anti-corruption compliance programs often involve collecting and using information about individuals to perform background checks, scrutinize red flags, or conduct internal investigations, these programs fall within the scope of the privacy and data protection laws. In order to carry out such activities lawfully, a company conducting due diligence on third parties may be required to notify concerned individuals about the company's privacy practices, obtain their consent to the collection and use of the personal information, establish agreements or other controls to share the personal information with affiliates and service providers, or obtain approvals from privacy regulators. Thus, performing adequate anti-corruption due diligence while respecting privacy obligations can be challenging, but can be accomplished.

Anti-Corruption Compliance

Anti-corruption laws of various countries, including the FCPA and the U.K. Bribery Act, criminalize bribing foreign government officials and create certain compliance obligations for global companies—even in jurisdictions that do not have their own anti-corruption laws.[3]

In a recent speech to a room full of compliance officers and practitioners, then Assistant Attorney General Lanny A. Breuer emphasized that the U.S. regulators' ''FCPA enforcement is stronger than it's ever been—and getting stronger.''[4] In the last two years alone, the Department of Justice (DOJ) has charged over 50 individuals with FCPA-related offenses and has collected nearly $2 billion in penalties.[5] Breuer made clear, however, that the United States is not alone in its fight against corruption. He discussed the proliferation of anti-bribery laws throughout the world and the growing and coordinated effort by various governments to combat bribery. As Breuer said, the FCPA is ''our way of ensuring not only that the [DOJ] is on the right side of his-

[1] Foreign Corrupt Practices Act of 1977, 15 U.S.C. §§ 78dd-1, et seq.

[2] Bribery Act, 2010, c. 23 (U.K.), *available at* http://www.legislation.gov.uk/ukpga/2010/23/contents/enacted.

[3] *See, e.g.*, 15 U.S.C. § 78dd-1(g); Bribery Act, 2010, c. 23, § 12 (U.K.).

[4] Assistant U.S. Attorney General Lanny A. Breuer, Speech at the Dept. of Justice 24th National Conference on the Foreign Corrupt Practices Act (Nov. 16, 2010), *available at* http://www.justice.gov/criminal/pr/speeches/2010/crm-speech-101116.html.

[5] *Id.*

 ISSN 1538-3423

tory, but also that it has a hand in advancing that history.''[6]

Against this background of aggressive anti-corruption compliance enforcement, there has been a dramatic change in the way global companies think about compliance. More multinational companies are adopting best practices to comply with anti-corruption laws, including the adoption of comprehensive policies and procedures addressing bribery risks.

One common risk that compliance programs should address is the use of third parties, such as consultants, agents, distributors, and other business partners. After all, under such laws as the FCPA and the U.K. Bribery Act, the fact that a bribe is paid by a third party does not eliminate the potential for criminal or civil liability. Rather, under certain circumstances, a company can be held liable for the actions of its third parties. For this reason, companies should vet the third parties they work with and do their utmost to know with whom they are doing business.

Due Diligence Processes

Companies should conduct an appropriate level of risk-based due diligence of potential third parties. Just what degree of due diligence is necessary varies based on the particular risk factors, including the type of services the third party will be providing, the industry, the countries and regions involved, the size and nature of the transaction, and the historical relationship with the third party. The aim of the due diligence is to attempt to determine whether business partners and commercial intermediaries are reputable, and to assess whether or not they are engaged (or could become engaged) in making illicit payments.

Due diligence processes are designed to collect, typically through questionnaires, information that is then checked against commercially or publicly available watch lists, databases, news archives, or other sources. The questionnaires and other vetting measures usually seek information not only about the commercial entity, but also about its principals and other key personnel. As a result, companies often collect information about individuals' financial accounts, history of criminal activity, including bribery or related activities, debarments, inclusion on a public watch list, and business or personal relationships with government officials. While companies are making efforts to comply with the anti-corruption laws, given the nature of the questions being asked, companies also need to consider compliance with applicable privacy and data protection laws.

Privacy Challenges

Specific provisions of privacy and data protection laws can vary widely, but there are common elements to many laws.

Notice Requirements

Many privacy laws require persons who collect, use, and share personal information to provide notice to the individuals concerned. A company conducting due diligence therefore may bear the responsibility for providing notice to the individuals whose information it collects as part of the due diligence process, even if the information comes from a central contact at the entity being scrutinized or from an external due diligence provider. Commonly, a notice must include details about what the company is doing with the personal information, including: what information is collected; the purpose(s) for which the information is collected and used; the identity of the company using the information; whether information will be disclosed to third parties (e.g., affiliates or foreign governments), and if so, to whom; the individual's right to access and correct the information and to object to the use of his/her personal information; and whether the personal information will be shared ''cross-border'' (i.e., beyond the borders of the country in which it was collected). Furthermore, individuals should be informed if third-party sources will provide personal information about them.

Consent Requirements

In addition to providing notice, a company conducting due diligence may need to obtain consent from the individuals concerned to collect, use, disclose, and transfer their personal information cross-border. Like the obligation to give notice, consent requirements (e.g., whether consent is required and the form it must take) vary from country to country.

Restrictions on Certain Sensitive Information

Privacy laws often aim to protect the very information that a due diligence process is seeking to uncover. An individual's political affiliations, and the information from which his or her political opinions can be derived, are deemed sensitive data under many countries' privacy laws. Information about an individual's criminal history or interactions with the justice system is also considered very sensitive in many countries; judicial information generally encompasses criminal prosecutions and convictions, an individual's being suspected of or investigated for committing a crime, and administrative or criminal sanctions imposed on an individual. This amounts to a broad realm of sensitive information, for which privacy laws often require the individual's express written consent and, in some countries, other heightened protections. While not intended to be a complete list, below are a few of the additional obligations that may be required:

- In Germany, companies may collect criminal data about individuals only if required to do so by an EU statute; where such an obligation exists, the information can only be collected in the form and manner prescribed by German law.[7]
- In France, companies must obtain the data protection regulator's prior authorization to collect and use criminal and judicial history information.[8]

[6] *Id.*

[7] Bundesdatenschutzgesetz (BDSG) [Federal Data Protection Act], Jan. 14, 2003, Bekanntmachung (BGBI.) [Federal Law Gazette 1, p. 66], at pt. III (Ger.).

[8] Loi 78-17 du 6 janvier 1978 modifiée [Law 78-17 of Jan. 1978, modified], Journal Officiel de la Republique Francaise [J.O.] [Official Gazette of France], *last amended and reprinted in* Journal Officiel du 26 aout 2011 [J.O. Aug. 26, 2011], at art. 26.

  PVLR ISSN 1538-3423

- In Italy and Greece, prior authorization from the data protection authority is required to collect and use any sensitive data.[9]
- In addition to requiring the regulator's approval, Austrian law prohibits the cross-border transfer of criminal history information in personally identifiable form unless the company has a sufficient justification for doing so; compliance with non-EU anti-corruption laws does not suffice.[10]
- In Poland, employers cannot collect, use, or share criminal record information about employees, so third-party intermediaries undergoing due diligence are unable to provide relevant information, even if they are willing and even if their employees consent to its use.[11]
- In Russia and Uruguay, only competent public agencies or persons designated by law are permitted to collect and use criminal history information.[12]

Compliance Recommendations

While building a due diligence process to comply with anti-corruption laws, organizations should consider the following points to remain compliant with privacy laws:

- **Draft notices that are comprehensive, but not overly broad.** Overly broad notices may be rejected by local regulators as insufficient, but organizations should draft notices that address the foreseeable ways in which the personal information may be used as a result of the due diligence. For example, the company should ensure that it can rely on the notice given to individuals if due diligence on a third-party intermediary currently acting on the company's behalf uncovered a need to conduct an investigation and to share information with forensic analysts or government agencies. The company will likely need the third party's cooperation to convey the notice to affected individuals, so it should fully inform the third party about its handling of the personal information.
- **Have a strategy for dealing with consent.** While it may not be feasible to obtain consent from each individual on whom due diligence is conducted, the company should make an effort to ensure that individuals have consented where necessary. Such efforts can include, for example, obtaining certifications and other contractual guarantees from the third party providing the information, or periodically requesting to see copies of the consents received by the third party.
- **Carefully formulate due diligence questions to comply with local limitations on sensitive data collection.** In drafting questions concerning criminal or judicial history, or associations with government officials, companies should aim to solicit answers that are proportional to the purpose of the due diligence. Questions asking whether key personnel are government officials or have some association with government officials must be carefully phrased to avoid treading into political opinion territory. Ideally, answers should be limited to information relevant and necessary for the screening. If acceptable from a risk perspective, companies should avoid obtaining judicial information related to identifiable individuals. Remember that a one-size-fits-all approach will not work. The due diligence questionnaires will need to be tailored to particular jurisdictions, and the same questionnaire may not work for all countries involved.

Privacy and data protection laws may prescribe other types of obligations or limitations in addition to the ones described above. For example, some laws may require a certain level of security to protect the collected information. Also, if a company intends to consolidate due diligence information from multiple countries into a centralized database, it must comply with legal requirements related to cross-border transfers. This may include filing registrations with privacy regulators, and executing data transfer agreements with affiliates and service providers that will have access to the data. Again, the requirements vary from country to country, and companies should allot sufficient time and resources to plan a coordinated approach to privacy obligations.

Conclusion

In today's regulatory climate of aggressive anti-corruption compliance enforcement, global companies should implement policies and procedures tailored to their risks in order to minimize exposure to liability. This includes implementing third-party due diligence procedures in order to ensure companies know with whom they are doing business.

In their efforts to comply with the anti-corruption laws, however, companies should carefully consider compliance with applicable privacy and data protection laws. While there may appear to be tension between these laws, the challenges of compliance with both anti-corruption laws and privacy and data protection laws are not insurmountable. More and more companies are meeting these challenges and successfully harmonizing the requirements of the anti-corruption laws and the privacy and data protection laws.

[9] Decreto Legge de 30 June 2003, n. 196 (It.) [Personal Data Protection Code, Legislative Decree No. 196], June 30, 2003, § 26; Nomos 2472/1997 [Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (as amended)] (Greece), at art. 7.

[10] Bundesgesetz ber den Schutz personenbezogener Daten [Federal Act concerning the Protection of Personal Data], Bundesgesetzblatt I [BGBl.], No. 165/1999, § 13 (Austria) as amended at BGBl I No. 112/2011.

[11] [Act of August 29, 1997 on the Protection of Personal Data], [Journal of Laws of July 6, 2002, No. 101, item 926], at art. 27 (Poland).

[12] [Federal Law of 27 July 2006 N 152-FZ on Personal Data], § 10 (Russia); Ley de Protección de Datos Personales y Acción de Habeas Data [Law on the Protection of Personal Data and Habeas Data Action], No. 18.331 (2008) (Uruguay).

Suhna Pierce is an associate with the Global Privacy and Data Security practice in Morrison & Foerster's New York City office, where she assists clients in complying with U.S. and foreign privacy and data protection laws. Ruti Smithline is a partner in the Litigation Department of Morrison & Foerster's New York City office and a member of the Securities Litigation, Enforcement, and White-Collar Practice Group. Smithline is a member of the firm's FCPA + Anti-Corruption Task Force and has also advised clients on FCPA compliance programs. Marian Waldmann Agarwal is an associate with the Global Privacy and Data Security practice in Morrison & Foerster's New York City office, where she counsels clients regarding the collection, use, disclosure, and transfer of personal information as organizations seek to comply with U.S. and international privacy and data protection laws.

  PVLR ISSN 1538-3423