MORRISON | FOERSTER

Morrison & Foerster Client Alert.

December 3, 2012

Anti-Corruption and Privacy Laws – Collision Course?

By Suhna Pierce, Marian Waldmann and Ruti Smithline

More and more companies are implementing due diligence processes for engaging third parties. Although companies adopt these processes in order to reduce the risks of violating anti-corruption laws, such as the U.S. Foreign Corrupt Practices Act ("FCPA") and the UK Bribery Act 2010 ("UK Bribery Act"), their due diligence programs may unwittingly expose them to risks under privacy and data protection laws around the world. Complying with both anti-corruption and privacy laws can be challenging, but can be accomplished.

Anti-corruption laws of various countries, including the FCPA and the UK 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.

In a recent speech to a room full of compliance officers and practitioners, Assistant Attorney General Lanny A. Breuer emphasized that the U.S. regulators' "FCPA enforcement is stronger than it's ever been—and getting stronger."[1] 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. Mr. Breuer made clear, however, that the U.S. 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 Mr. Breuer said, the FCPA is "our way of ensuring not only that the [DOJ] is on the right side of history, but also that it has a hand in advancing that history."

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 UK Bribery Act, the fact that a

[1] *See* Stacey Sprenkel, FCPA Regulators Speak on Newly Released FCPA Guidance and Reiterate Unwavering Commitment to FCPA Enforcement, Client Alert (Nov. 20, 2012).

Beijing
Jingxiao Fang 86 10 5909 3382
Paul D. McKenzie 86 10 5909 3366

Brussels
Joanna Łopatowska 32 2 340 7365
Karin Retzer 32 2 340 7364

Hong Kong
Eric Dickinson 852 2585 0812
Gordon A. Milner 852 2585 0808

London
Ann Bevitt 44 20 7920 4041
Deirdre Moynihan 44 20 7920 4164
Anthony Nagle 44 20 7920 4029

Los Angeles
Michael C. Cohen (213) 892-5404
David F. McDowell (213) 892-5383
Purvi G. Patel (213) 892-5296
Russell G. Weiss (213) 892-5640

New York
Madhavi T. Batliboi (212) 336-5181
John F. Delaney (212) 468-8040
Matthew R. Galeotti (212) 336-4044
Sherman W. Kahn (212) 468-8023
Mark P. Ladner (212) 468-8035
Michael B. Miller (212) 468-8009
Suhna N. Pierce (212) 336-4150
Marian A. Waldmann (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Northern Virginia
Daniel P. Westman (703) 760-7795

Palo Alto
Christine E. Lyon (650) 813-5770
Bryan Wilson (650) 813-5603

San Francisco
Roland E. Brandel (415) 268-7093
Anna Ferrari (415) 268-6728
Jim McCabe (415) 268-7011
James R. McGuire (415) 268-7013
William L. Stern (415) 268-7637

Tokyo
Daniel P. Levison 81 3 3214 6717
Gabriel E. Meister 81 3 3214 6748
Jay Ponazecki 81 3 3214 6562
Toshihiro So 81 3 3214 6568
Yukihiro Terazawa 81 3 3214 6585

Washington, D.C.
Nicholas A. Datlowe (202) 887-1590
Richard Fischer (202) 887-1566
D. Reed Freeman, Jr. (202) 887-6948
Julie O'Neill (202) 887-8764
Obrea O. Poindexter (202) 887-8741
Cynthia J. Rich (202) 778-1652
Robert A. Salerno (202) 887-6930
Andrew M. Smith (202) 887-1558
Nathan David Taylor (202) 778-1644

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, typically through questionnaires, are designed to collect 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

Because due diligence programs involve the collection of information about individuals, these programs fall within the scope of privacy and data protection laws in many jurisdictions that regulate the collection and use of personal information. More than 70 countries worldwide currently have a privacy or data protection law. Under these laws, personal information generally means any information pertaining to identified or identifiable individuals.

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

The 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 as comprehensive, 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.
- In France, companies must obtain the data protection regulator's prior authorization to collect and use criminal and judicial history information.
- In Italy and Greece, prior authorization from the data protection authority is required to collect and use any sensitive data.
- 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.
- In Poland, employers cannot collect, use, and 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.
- In Russia and Uruguay, only competent public agencies or persons designated by law are permitted to collect and use criminal history information.

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 as insufficient by local regulators, 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 could 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 likely will 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 could 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.

Morrison & Foerster's FCPA + Anti-Corruption Task Force:

Paul T. Friedman
San Francisco
(415) 268-7444
pfriedman@mofo.com

Timothy W. Blakely
Hong Kong
+ 852 2585 0870
tblakely@mofo.com

Randall J. Fons
Denver
(303) 592-2257
rfons@mofo.com

Daniel P. Levison
Tokyo
+ 81 3 3214 6717
dlevison@mofo.com

Carl H. Loewenson, Jr.
New York
(212) 468-8128
cloewenson@mofo.com

Kevin Roberts
London
+ 020 7920 4160
kroberts@mofo.com

Robert A. Salerno
Washington, D.C.
(202) 887-6930
rsalerno@mofo.com

Ruti Smithline
New York
(212) 336-4086
rsmithline@mofo.com

Rick Vacura
Northern Virginia
(703) 760-7764
rvacura@mofo.com

Sherry Yin
Beijing
+ 86 10 5909 3566
syin@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's A-List* for nine straight years, and *Fortune* named us one of the "100 Best Companies to Work For."

Client Alert.

Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law*," or our free online Privacy Library, please visit: http://www.mofo.com/privacy--data-security-services/ and "like" us on Facebook at http://www.facebook.com/MoFoPrivacy.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.