TABLE OF CONTENTS

I. International Risk
   a. DOJ Publishes New Guidance for Compliance Programs
   b. Forecasting International Risk Climate Under President Trump
   c. $519 million FCPA Payment by Teva Pharmaceuticals – Largest Ever FCPA Payment by a Pharmaceutical Company – Follows Large FCPA Plea Agreement with Odebrecht and Braskem
   d. Mondelēz Agrees to Pay $13 Million to Settle FCPA Charges Related to Inadequate Due Diligence and Accounting Controls over Third Party in India
   e. Hot Topics in Supply Chain Compliance
   f. Case Closed! – The Conflict Minerals Rule Litigation is Over, but the Drama Continues
   g. SEC Issues Updated Statement on Conflict Minerals Rule
   h. Evaluating the FCPA Pilot Program: The Data, The Trends

II. Privacy & Data Security
   a. Privacy Implications of President Trump’s Immigration Order
   b. The GDPR – Possible Impact on the Life Sciences and Healthcare Sections
   c. Cookies Crumble? The draft EU Regulation on Privacy and Electronic Communications
   d. Thoughts on EU’s Draft E-Privacy Regulation
   e. The Information Commissioner’s Guidance on Consent under the GDPR

III. Brexit
   a. Implications of the UK’s Brexit Referendum
   b. An Update on Brexit and the Implications for General Data Protection Regulation (GDPR)
   c. Brexit White Paper Published

IV. Asia
   a. China FDA Clarifies Legal Consequences of Clinical Trial Data Inspections
   b. Donations and Grants in China: Compliance Controls Beyond T&E
   c. Recent Developments in Japanese Enforcement of Foreign Bribery Laws
   d. China Solicits Comments on Drug GCP
e. CFA Amends Medical Device Recall Rules
f. Hong Kong Proposes Enhanced AML Obligations for Professionals and Beneficial Owner Registries for Hong Kong Companies
g. China’s State Council Announces Major Policies to Reform the Pharmaceutical Industry
h. U.S. Department of Commerce Establishes Favorable Export Control Policies for India
i. South Korea Fines Prominent Pharmaceutical Manufacturer in Latest Anti-Corruption Enforcement Efforts

V. European Union, Middle East, Africa
   a. European Health Care Compliance Challenges (And Solutions)
   b. EU Reaches Final Agreement on Conflict Minerals Regulation – An Overview
   c. The UK Modern Slavery Act – A Compliance Primer for Fund Managers

VI. Latin America
   a. Mexico Enacts a Sweeping New Anti-Corruption Regime, Accompanied by a Public Apology from President Peña Nieto and Increased Attention on Mexico’s Energy Sector by U.S. Regulators
   b. Top 10 Anti-Corruption Red Flags in Latin America
   c. Update on the Anti-Corruption Landscape in Mexico
   d. A Judicial Reinterpretation of the Brazilian Constitution’s Right to Health Care
March 1, 2017

**DOJ Publishes New Guidance for Compliance Programs**

On February 8, 2017, the Fraud Section of the U.S. Department of Justice (the “DOJ”) published a guide for companies called “Evaluation of Corporate Compliance Programs” (the “Guidance”). The Guidance is composed of common questions that the DOJ asks when evaluating a company’s compliance program. While the Guidance questions are largely based on familiar sources, such as the United States Sentencing Guidelines and the “Principles of Federal Prosecution of Business Organizations” in the United States Attorney’s Manual,¹ the questions provide a greater degree of detail and insight into the DOJ’s process for evaluating compliance programs.

**Areas Covered**

The Guidance focuses on three overarching areas: (1) company culture, (2) compliance structure and resources, and (3) the effectiveness of company policies and procedures.

Regarding company culture, the Guidance questions focus on the behavior of senior and middle management. The Guidance asks whether management and company leaders have encouraged or discouraged the misconduct in question, and whether their actions have demonstrated a commitment to ensuring compliance. Further, the Guidance inquires into the responsiveness of management to compliance concerns and the remedial steps taken after misconduct was discovered. The Guidance also asks whether management has incentivized compliance and ethical behavior, and whether the company has considered any potential negative compliance implications of its business model and incentive structure.

Second, the Guidance lists questions related to the company’s compliance structure and resources. The Guidance inquires into the lines of communication that employees may use to convey compliance concerns to the board of directors and senior management, as well as the compliance structure’s role in the company’s strategic and operational decisions. Moreover, the Guidance clearly expects companies to employ experienced and qualified compliance personnel and allocate appropriate resources and funding to compliance-related items, such as internal audits, periodic control testing, and frequent updates to assessment procedures.

Last, the Guidance engages with the company’s compliance policies and procedures. The Guidance asks detailed questions about the design, accessibility, and integration of the company’s policies. The Guidance also evaluates how employees are trained on company policies and procedures, and how the policies operate to ensure compliance in the context of mergers, acquisitions, and third-party management. Ultimately, the Guidance takes a multi-dimensional look at the effectiveness of the company’s policies and procedures, rather than how they are written or crafted.

**Key Takeaways**

Although the content of the Guidance is largely familiar to practitioners, it does give a clearer picture of the DOJ’s current approach to corporate compliance. The issuance of the Guidance underscores the DOJ’s renewed focus on the operation, rather than the appearance, of corporate compliance programs.

Additionally, while the document is framed as guidance for companies, as opposed to a checklist or formula for compliance, the clear import of the Guidance is that companies will be asked detailed and challenging questions.

---

¹ The Guidance pulled topics and questions from various other sources, including DOJ corporate resolution agreements, DOJ and SEC publications, and publications from the Organization for Economic Cooperation and Development.
regarding the scope and effectiveness of their compliance programs. Accordingly, companies will need to seriously consider how their programs will withstand such scrutiny, or risk the possible consequences of loss of credit for their compliance programs, higher penalties, or even separate violations for inadequate internal controls.

For more information, please feel free to contact a member of Ropes & Gray’s leading anti-corruption / international risk and government enforcement teams.
November 15, 2016

Forecasting International Risk Climate Under President Trump

The article by international risk counsel Michael Casey, international risk practice co-chair Zachary Brez and associate Brendan Hanifin was originally published in Law360 on November 13, 2016.

Niels Bohr famously observed that “predictions are hard, especially about the future.” The results of last week’s presidential election confirmed this adage, as prognosticators in the media, both political parties, and the financial and legal industries seemingly all failed to envisage Donald Trump’s victory. The aftermath of the election has indicated that a corollary to Bohr’s maxim also is true: commentators of all stripes will continue to try to forecast the future, regardless of the difficulty of doing so. In this article, we offer our best guesses about potential regulatory and enforcement changes that might occur in the international risk landscape after Inauguration Day.

I. Iranian Sanctions

On January 16, 2016 (“Implementation Day”), the United States and the European Union lifted or amended many nuclear proliferation-related sanctions against Iran pursuant to the Joint Comprehensive Plan of Action (“JCPOA”). The United States eliminated most of its secondary sanctions, and also scaled back certain parts of its primary sanctions regime. Most notably, the Office of Foreign Assets Control (“OFAC”) within the U.S. Department of Treasury issued a general license (“General License H”) that permits foreign entities owned or controlled by U.S. companies (“Foreign Entities”), including foreign subsidiaries of U.S. companies and foreign portfolio companies of U.S. private equity sponsors, to conduct business with Iran, subject to various restrictions. The European Union significantly scaled back its sanctions against Iran as part of the JCPOA, and General License H permits, to some extent, Foreign Entities to compete alongside European companies to win new business in Iran.

During the election campaign, Mr. Trump sharply criticized the JCPOA. After becoming President, Mr. Trump could end the United States’ participation in the JCPOA. But as the JCPOA was negotiated in partnership with five other countries, it seems unlikely that President Trump would withdraw the United States from the JCPOA in its entirety. A more plausible scenario is that President Trump may undo certain aspects of the sanctions relief that the United States has granted Iran since Implementation Day, such as revoking General License H. This act alone would have significant consequences, as many Foreign Entities have spent significant time and money establishing policies and procedures designed to ensure compliance with General License H, developing relationships with Iranian counterparties, and even making capital investments in Iran. Some companies have approached new business opportunities in Iran cautiously, while others have jumped more aggressively. Regardless, a forced and time-limited wind-down of Iranian business dealings would impose financial and operational costs for even the best-prepared companies.

Alternatively, the Trump administration might accuse Iran of violating its obligations under the JCPOA, potentially resulting in the “snap back” of all of the U.S. sanctions that were in place prior to Implementation Day. This strategy—which Mr. Trump foreshadowed during an August 2015 interview (“I would police that contract so tough that they don’t have a chance”)—may earn President Trump the approbation of Republican lawmakers, many of whom vigorously opposed the JCPOA and favored imposing additional, new sanctions on Iran.
II. Russian Sanctions

Following Russia’s annexation of Crimea in March 2014, President Barack Obama issued an executive order authorizing the Treasury Department to impose sanctions on individuals and entities that operate in certain sectors of the Russian economy. Pursuant to the executive order, OFAC has issued sectoral sanctions targeting Russian financial institutions, defense companies, and energy firms. In addition, OFAC has targeted a number of persons in Russian President Vladimir Putin’s inner circle with list-based sanctions and imposed comprehensive sanctions on the Crimea region of Ukraine. The European Union imposed sanctions that are similar to the measures imposed by OFAC.

The European Union responded to the annexation of Crimea by Russian forces in a similar way and imposed sanctions against Russian and Crimean entities and individuals that are broadly similar to the measures imposed by OFAC. Russia’s response to these European sanctions has been to impose a ban on certain food and agricultural products from European countries.

Mr. Trump has indicated that he wishes to improve U.S. relations with Russia and both Mr. Trump and President Putin have spoken with apparent admiration for each other. In Europe, where the continuation of sanctions against Russia in 2017 will require the approval of all 28 Member States, there are signs that countries such as Italy, Cyprus and Greece favor relaxing some or all of the current sanctions in place. Many other European countries, however, have made it clear that they are unwilling to relax sanctions until Russia has demonstrated improved compliance with the Minsk Agreement, which calls for a cessation of hostilities in eastern Ukraine. Senior U.S. government officials in the Obama administration—including Secretary of State John Kerry—also have expressed skepticism about the continuing utility of at least some of these sanctions.

Against this backdrop, President Trump may unilaterally elect to end the U.S. sanctions on Russia, irrespective of contrary views expressed by NATO allies in Europe. Alternatively, he could seek to engage the Kremlin in negotiations over sanctions relief in exchange for (1) increased cooperation with respect to the ongoing Syrian conflict and/or (2) Russia's agreement to reverse its military buildup in the Baltic region. Indeed, both President Putin and President Trump may view a negotiated solution as politically expedient. President Putin would achieve the lifting (or relaxation) of sanctions that have damaged the Russian economy, and Mr. Trump could claim that he defused an inherited political crisis.

III. Cuban Sanctions

Since December 2014, President Obama has significantly changed the United States’ policy toward Cuba through modifications to the Cuban Asset Control Regulations and the Export Administration Regulations. These changes have created significant new opportunities for U.S. companies and some foreign companies to engage in certain types of business in and with Cuba and to export particular types of U.S.-origin products to Cuba. With the most recent amendments to the Cuban Assets Control Regulations, announced in October 2016, President Obama has taken virtually every step within his authority to relax the Cuban embargo; any further loosening—or the termination of—the Cuban sanctions would require Congressional action (for which there appears to be limited political appetite).

During the election campaign, Mr. Trump pledged to “reverse” President Obama’s executive orders related to Cuba, thereby reverting to the U.S. policy of non-engagement that prevailed from the early 1960s through 2014. This shift in U.S. policy toward Cuba would represent a significant setback for U.S. companies—including airlines and hospitality companies—that have made sizeable investments in anticipation of increased engagement with Cuba.

---

1 Even with these recent changes, primarily accomplished via executive orders, the Cuban sanctions continue to prohibit most transactions by U.S. companies (as well as U.S. companies’ foreign subsidiaries) involving Cuba.
IV. Scrutiny of Foreign Investors and Investments in the United States

Throughout his campaign, Mr. Trump repeatedly denounced the impact of foreign government and foreign commercial interests on the U.S. economy. One way in which President Trump may seek to address these perceived problems is by mandating increased scrutiny of prospective foreign investors and investments through the Committee on Foreign Investment in the United States (“CFIUS”) and Defense Security Service (“DSS”) review processes.2

After Mr. Trump becomes President, CFIUS might have the authority to review a wider range of transactions. Indeed, during the last few months, some (mostly Republican) Congress members have sought to increase the scope of CFIUS’s power in order to allow the interagency committee to address perceived national security concerns more effectively. Mr. Trump’s victory increases the likelihood that CFIUS’s power will be expanded.

Even if CFIUS’s or DSS’s jurisdiction remains the same, each may adopt a more aggressive approach when reviewing relevant transactions. Importantly, CFIUS and DSS each exercise considerable discretion in reviewing transactions within their jurisdiction. The Trump administration may encourage increased scrutiny of proposed transactions involving foreign entities, which, in turn, may result in CFIUS blocking more covered transactions and DSS imposing more onerous mitigation measures on transactions that result in U.S. companies coming under foreign ownership or control. Based on comments made during Mr. Trump’s campaign, it seems possible that CFIUS and DSS could take a particularly hard look at transactions involving foreign investors from China.

V. Conclusion

During his campaign, Mr. Trump signaled dramatic changes to U.S. foreign policy that, if implemented, could produce significant financial, operational, and compliance-related consequences for U.S. and international companies. While it is too early to assess the impact of a Trump presidency on U.S. foreign policy, the next 70 days present an opportunity for companies to consider how to respond to the potential changes outlined above.

---

2 CFIUS is an interagency committee of the U.S. government authorized to review transactions that could result in control of a U.S. business by a foreign person. DSS is responsible for administering facility clearances (i.e., permission to access classified information of the U.S. government). When a foreign entity obtains a five percent or greater interest in a U.S. company that holds a facility clearance, the foreign entity’s interest must be reported to DSS, which may require the U.S. company to implement mitigation measures.
December 29, 2016

$519 million FCPA Payment by Teva Pharmaceuticals—Largest Ever FCPA Payment by Pharmaceutical Company—Follows Large FCPA Plea Agreement With Odebrecht and Braskem

Summary

On December 22, 2016, the world’s largest manufacturer of generic pharmaceuticals, Teva Pharmaceuticals (“Teva”), agreed to pay $519 million in FCPA-related criminal penalties, disgorgement, and interest. The Israeli company Teva entered into a deferred prosecution agreement with the U.S. Department of Justice (“DOJ”) to settle allegations that it had bribed government officials in Russia, Ukraine, and Mexico. Teva’s settlement is the fourth-largest Foreign Corrupt Practices Act (“FCPA”) settlement ever, and the largest-ever by a pharmaceutical company. The $519 million payment imposed on Teva is significantly higher than the next-highest FCPA-related payment imposed on a pharmaceutical company, $70 million imposed in 2011.

The Teva settlement came on the heels of Odebrecht and Braskem’s global $3.5 billion settlement with authorities in the United States, Brazil, and Switzerland, announced the day before, on December 21, 2016. The Brazilian-based construction company Odebrecht pleaded guilty to a conspiracy to violate the FCPA, with the fine to be determined in the future at sentencing on April 17, 2017. Braskem, Odebrecht’s petrochemical unit, also pleaded guilty.

Teva: Bribes to Government Officials and Inadequate Internal Controls

The Teva agreement detailed the company’s payment of bribes to government officials in Russia, Ukraine, and Mexico, and the company’s lack of internal controls to prevent bribery.

In Russia, Teva executives and employees bribed a high-ranking government official in order to increase sales of Teva’s multiple sclerosis drug Copaxone, one of Teva’s most profitable products. The Russian government official influenced the Russian Ministry of Health’s annual drug purchase auctions to increase Copaxone sales. In return, Teva employed the Russian government official’s drug repackaging and distribution company. From 2010 until at least 2012, he earned approximately $65 million through inflated profit margins to his company.

In Ukraine, Teva also bribed a senior Ukrainian Ministry of Health official to influence Ukraine’s approval of Teva’s drug registrations, including those of Copaxone and insulins. These drug registrations were necessary to market and sell products within Ukraine. From 2001 to 2011, Teva employed the official as a “registration consultant,” paying him a monthly fee along with other items of value, including travel, totaling approximately $200,000.

In Mexico, Teva’s Mexican subsidiary bribed doctors starting in at least 2005 to prescribe Copaxone. Teva became aware of these bribes in 2009, when the company was developing its anti-corruption compliance program. Despite this awareness, Teva approved and implemented an anti-bribery compliance program that could neither prevent nor detect bribes. Additionally, compliance managers were put in place who either could not or would not enforce Teva’s anti-corruption policies.
Teva: Deferred Prosecution Agreement Accounts for “Substantial Cooperation and Remediation”

The U.S. government’s investigation of Teva began in 2012 with a U.S. Securities and Exchange Commission (“SEC”) subpoena. Teva learned of its FCPA problems that same year, and immediately took steps to address the problems. In 2012, Teva voluntarily began a comprehensive investigation into its global operations and named a global head of compliance. Teva engaged independent counsel to conduct a global corruption risk assessment. In 2013, Teva replaced its entire Russian leadership team. Teva no longer employs the individuals involved in the bribes.

On December 22, 2016, Teva entered into a deferred prosecution agreement (“DPA”) with the DOJ, agreeing to pay criminal penalties of approximately $283 million. The DPA requires that Teva work with an independent compliance monitor for three years. Teva also agreed to pay the SEC approximately $236 million in disgorgement and pre-judgment interest. The DOJ charged the company with two counts: one of conspiracy to violate the FCPA and one of failing to implement adequate internal controls. Teva Russia pleaded guilty to one count of conspiracy to violate the FCPA.

Teva’s remediation efforts were noted by the DOJ, including (1) terminating employees, (2) enhancing compliance, (3) improving anti-corruption training, (4) adopting a stand-alone third-party due diligence program, (5) making Teva’s control functions more independent and establishing an office to address reports of misconduct, and (6) strengthening the internal audit and investigations teams.

While the DOJ reduced Teva’s criminal penalty by 20% from the bottom of sentencing guidelines because of “substantial cooperation and remediation,” Teva did not get the largest possible reduction due to actions that delayed the government’s investigation, including “overbroad assertions of attorney-client privilege” and slow responses to document requests. Additionally, Teva did not get any credit for self-disclosing.

Odebrecht & Braskem: Bribery of Politicians and Political Parties

The December 21, 2016 settlement with Odebrecht and Braskem was part of “Operation Car Wash,” a long-running investigation by Brazil prosecutors into corruption at Petrobras, Brazil’s state energy company. Earlier in 2016, Odebrecht’s CEO had been sentenced to 19 years imprisonment.

Odebrecht admitted to a bribery and bid-rigging scheme that started as early as 2001, through which the company paid approximately $788 million in bribes to government officials and political parties in many countries. The bribes were directed by company management and were paid using shell companies, off-shore bank accounts, and off-book transactions. A dedicated department within Odebrecht, the “Division of Structured Operations,” administered these bribes. The Division of Structured Operations had an entirely separate off-books communications system that allowed communication using codenames and passwords via secure emails and instant messages.

As Odebrecht’s petrochemical unit, Braskem contributed about $250 million to Odebrecht’s bribe system. This money ended up with Brazilian politicians and political parties, as well as with a Petrobras official. In exchange, Braskem received benefits that included contracts with Petrobras, preferential rates for the purchase of Petrobras’ raw materials, and favorable legislation reducing Braskem’s Brazil tax liabilities.

On December 21, 2016, Odebrecht and Braskem settled with the DOJ, Brazil’s Ministerio Publico Federal, and Switzerland’s Office of the Attorney General. The plea agreements require that the companies employ an independent compliance monitor for three years. The agreements accounted for the companies’ failure to voluntarily disclose; the nature and seriousness of the offenses, which involved the highest levels of the companies, lasted many years, and occurred in multiple countries; and the lack of an effective compliance and ethics program at the time of the offenses.
Odebrecht agreed that the appropriate criminal penalty would be $4.5 billion, but the company has claimed it can only pay $2.6 billion. The penalty will be determined during sentencing on April 17, 2017. Eighty percent of Odebrecht’s penalty will go to Brazil, with the United States and Switzerland each receiving 10 percent. Braskem pled guilty to one count of conspiring to violate the FCPA, agreeing to pay a $632 million criminal penalty. Braskem settled related charges with the SEC, agreeing to pay $325 million in disgorgement of profits. Seventy percent of Braskem’s penalty will go to Brazil, with the United States and Switzerland each receiving 15 percent. Between the penalties and the disgorgement, the United States will receive approximately $94.8 million from Braskem.

The companies’ remediation efforts were noted by the DOJ, including (1) disciplining and terminating employees, (2) heightening controls and compliance programs, and (3) “significantly increasing” compliance resources.

Odebrecht’s penalties were reduced by 25 percent from the bottom of sentencing guidelines as a result of Odebrecht’s “full cooperation,” and Braskem’s penalties were reduced by 15 percent from the bottom of sentencing guidelines as a result of Braskem’s “partial cooperation.”

Implication

With the Odebrecht, Braskem, and Teva payments, U.S. authorities will have imposed a record-setting $2.15 billion in FCPA-related payments in 2016, greatly exceeding the previous annual record for FCPA-related payments of $1.6 billion set in 2014. None of the companies voluntarily self-disclosed, and the U.S. government insisted that all three employ independent compliance monitors for three years. These settlements show that companies must cooperate promptly and completely in order to receive full financial credit for cooperation.
January 11, 2017

**Mondelez Agrees to Pay $13 Million to Settle FCPA Charges Related to Inadequate Due Diligence and Accounting Controls over Third Party in India**

On January 6, 2017, the U.S. Securities and Exchange Commission (“SEC”) announced that Illinois-based multinational confectionery company Mondelēz International Inc. and its subsidiary Cadbury agreed to settle Foreign Corrupt Practices Act (“FCPA”) charges relating to allegations of bribery in India. Mondelēz, formerly Kraft Foods Inc., and Cadbury will pay $13 million to settle the charges arising from payments Cadbury made to a consultant in India to obtain licenses and approvals for a chocolate factory. The SEC alleged due diligence failures by both Cadbury and Mondelēz. Allegedly, Cadbury failed to conduct adequate diligence on the consultant, whereas Mondelēz failed to conduct adequate diligence on Cadbury, both before and after acquiring the U.K. company.

**Resolution Details**

An SEC investigation concluded that, in 2010, Cadbury India retained a consultant to represent the company in interactions with the Indian government. Cadbury India paid the agent $90,666 over the course of six months. The services detailed in the agent’s invoices included drafting license applications for a chocolate factory Cadbury India planned to build in Baddi, India. Nevertheless, Cadbury employees, not the agent, prepared these license applications. Moreover, the agent withdrew most of the funds in cash upon receipt of each payment. One such approval designated the chocolate factory as two distinct units for tax purposes, resulting in approximately $85 million in tax benefits for Mondelez.

The SEC charged Mondelēz and Cadbury with violating the books-and-records and internal-controls provisions of the FCPA. Cadbury allegedly failed to maintain records that accurately reflected the nature and value of the services provided by the consultant. The SEC also found that Cadbury did not maintain internal accounting controls sufficient to reasonably prevent improper or unauthorized payments. Moreover, the SEC alleged that Cadbury failed to conduct appropriate due diligence on and monitor the activities of the agent, which created the risk that the funds could be used for improper or unauthorized purposes.

The SEC’s investigation also determined that parent company Mondelēz failed to perform adequate anti-corruption compliance diligence when it acquired Cadbury. Mondelēz acquired Cadbury on February 2, 2010, at the beginning of Cadbury’s relationship with the agent. Mondelēz did not conduct complete pre-acquisition due diligence, and its six-month post-acquisition due diligence did not identify the contemporaneous relationship between Cadbury and the agent. The SEC concluded that, as a result of Mondelēz’s acquisition of Cadbury, it is responsible for the subsidiary’s violations.

Mondelez discovered the relationship in October 2010 and commenced an internal investigation, which resulted in the termination of Cadbury’s relationship with the consultant. Mondelēz then implemented its global compliance program at Cadbury and comprehensively reviewed Cadbury India’s use of third parties in its business. Mondelēz did not disclose the potential violations, which were reported to the SEC by a whistleblower in 2015. The SEC’s settlement order, however, noted Mondelēz’s cooperation with the investigation.
A dispute with the Indian government over the tax designation remains ongoing.

**Key Takeaways**

This settlement illustrates the importance of several key principles for mitigating the anti-corruption risks associated with conducting business in high-risk markets:

- Perform robust anti-corruption due diligence prior to international acquisitions.
- Identify and monitor high-risk third-party relationships as part of a comprehensive compliance program.
- Demand accurate, itemized, and timely invoices and supporting documentation for all payments to third parties.

If you have any questions, please contact your usual Ropes & Gray advisor.
January 23, 2017

**Hot Topics in Supply Chain Compliance**

The last few years have seen a proliferation of new supply chain-focused regulations and other compliance obligations, a trend which isn’t likely to abate any time soon. In this Alert, we provide an overview of selected supply chain compliance items that should be on the radar screen of healthcare industry legal and compliance professionals in 2017.

**Anti-Human Trafficking**

Anti-human trafficking compliance is a newer area of focus for many healthcare companies as a result of recently adopted disclosure and compliance requirements and increasing stakeholder scrutiny.

*The UK Modern Slavery Act (MSA).* Starting this year, the MSA will require a significant number of healthcare companies to annually publish on their websites a statement describing the steps that they have taken during the preceding fiscal year to ensure that slavery and human trafficking are not taking place in any of their supply chains or in any part of their own businesses. This requirement applies to “commercial organisations” doing business in the United Kingdom, irrespective of home country, that provide goods or services and have worldwide turnover of at least £36 million.

Each company will need to tailor its statement to its particular risk assessment and compliance program. There are no mandatory topics that must be covered in the statement, although the MSA recommends that the following disclosure topics be addressed: (1) organizational structure, business model and supply chain relationships; (2) policies in relation to slavery and human trafficking; (3) slavery and human trafficking due diligence processes; (4) the parts of the business and supply chains where there is a risk of slavery and human trafficking taking place and the steps taken to assess and manage that risk; (5) the effectiveness in ensuring that slavery and human trafficking are not taking place in the business or supply chains, measured against appropriate key performance indicators; and (6) the training available to staff.

For additional Ropes & Gray resources describing the MSA in substantially more detail, including the statement requirement and action items for establishing a compliance program, see [here](#).

*The UK Labour Standards Assurance System (LSAS).* LSAS was commissioned by the UK Department of Health and NHS Supply Chain, which procures products for the National Health Service. LSAS is the foundation of NHS Supply Chain’s ethical procurement strategy. Initially introduced in 2012 in connection with its Framework Agreement for Surgical Instruments, NHS Supply Chain is introducing LSAS compliance into other contracts.

LSAS has 15 action points, including the following supply chain facing items: (1) adopting a labor policy for the supply chain that among other things addresses the use of child and forced labor; (2) assessing the extent to which labor standards are at risk of being abused within the supply chain; (3) communicating the policy and other relevant information to identified suppliers, collecting and verifying information relating to labor standards performance and responding to the information and evidence collected to drive continual improvement of labor standards throughout the supply chain.

There are four audit levels under LSAS, each of which requires a specified level of compliance with the LSAS action points: (1) Foundation - the vendor has begun to consider how labor standards relate to its business and there is some documentation in place for an auditor to review; (2) Implementation - the vendor has started to implement processes
and procedures to manage labor standards, including processes to identify risk in the supply chain; (3) Established -
the vendor has in place a robust system for managing labor standards and risk is being effectively mitigated where
uncovered; and (4) Progressive - the vendor demonstrates leadership level management of labor standards, going
beyond audit to tackle the root cause of issues and risks uncovered and is engaging with key stakeholders,
partnerships and projects to do so.

Suppliers must at a minimum be audited to Level 1/Foundation within six months of contract launch for NHS Trusts
to purchase supplies through NHS Supply Chain, with later deadlines to achieve compliance with higher LSAS
levels.

The US Federal Acquisition Regulation (FAR) Anti-Human Trafficking Provisions. The FAR governs the US
Federal government’s procurement process and applies to not only prime contractors, but in many cases
subcontractors and agents as well. The anti-human trafficking provisions of the FAR were significantly expanded in
March 2015. Because the amendments apply only to contracts and new task orders under existing indefinite
delivery/indefinite quantity contracts entered into after that time, the FAR anti-human trafficking compliance
requirements are only now starting to impact the compliance programs at many companies.

There are two principal compliance obligations under the FAR anti-human trafficking provisions. First, there are
nine prohibited activities applicable to contractors and subcontractors (which also includes indirect subcontractors)
and their employees and agents. This portion of the rule applies to all contracts.

Second, the FAR anti-human trafficking provisions require a compliance plan and periodic certifications if the
contract is for goods or services acquired or to be performed outside the United States with an estimated value that
exceeds $500,000. For purposes of calculating the dollar threshold, commercially available off-the-shelf items are
excluded.

Companies must design the compliance plan to fit their particular facts and circumstances. The compliance plan must
be appropriate to the size and complexity of the contract and the nature and scope of its activities, including the
number of non-US citizens expected to be employed and the risk that the contract will involve services or supplies
susceptible to trafficking in persons. In addition, the compliance plan must at a minimum include the following
elements: (1) an awareness program; (2) a grievance process; (3) a recruitment and wage plan that meets specified
requirements; (4) a housing plan, if the contractor or subcontractor intends to provide or arrange housing; and (5)
procedures to prevent violations and to monitor, detect and terminate agents, subcontractors or subcontractor
employees that have engaged in prohibited activities.

If required, certifications must be provided in connection with the contract award and annually. The contractor must
certify that: (1) a compliance plan and procedures to prevent prohibited activities and to monitor, detect and
terminate a contract with a subcontractor or agent engaging in prohibited activities have been implemented; and (2)
after having conducted due diligence, either, to the best of the contractor’s knowledge and belief, there have been no
occurrences of prohibited activities or, if they have occurred, appropriate remedial and referral actions have been
taken.

For more information on the FAR anti-human trafficking rule, see our Alert here.

Trade Facilitation and Trade Enforcement Act. This Act, which was adopted in early 2016, repealed the
“consumptive demand” exception to the US Tariff Act. The Tariff Act bans the importation of foreign goods and
merchandise produced or manufactured in whole or in part by convict, forced or indentured labor. However, under
the consumptive demand exception, the prohibition did not apply to the extent that US demand exceeded domestic
supply.
Since the adoption of the Act, several shipments of goods from China have been detained by US Customs and Border Protection for having been produced using forced labor. For purposes of assessing risk, commodities and products used in the healthcare industry appear on both the Department of Labor’s List of Goods Produced by Child Labor or Forced Labor and its List of Products Produced by Forced or Indentured Child Labor. Over time, third party tips alleging convict, forced or indentured labor in supply chains are likely to increase, which will put additional pressure on pre-emptive supply chain mapping for at-risk commodities and products.

**Proposed French Human Rights Legislation.** During November 2016, the French National Assembly adopted a bill that would require large French companies to adopt a vigilance plan to identify and prevent serious human rights violations, including at the subcontractor and supplier level. Requirements of the vigilance plan would include: (1) risk mapping; (2) procedures for assessing subsidiaries, subcontractors and suppliers; (3) risk mitigation; (4) a reporting and grievance mechanism drawn up in consultation with representative trade union organizations; and (5) a mechanism for monitoring the compliance measures implemented and evaluating their effectiveness. If adopted into law, this legislation will impact the supply chains of large French companies, including those in the healthcare industry, irrespective of where the supplier is located.

**Conflict Minerals**

Conflict minerals regulation will continue to be dynamic in 2017.

**US Conflict Minerals Rule.** The Conflict Minerals Rule was adopted pursuant to the Dodd-Frank Act. The Rule requires US public companies that manufacture or contract to manufacture products that contain tin, tantalum, tungsten or gold (3TG) to, among other things: (1) make supply chain inquiries to determine the source of the 3TG in their in-scope products; (2) if the 3TG originated or there is reason to believe may have originated in the Democratic Republic of the Congo region, conduct due diligence in accordance with the Organisation for Economic Co-operation and Development’s Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas; and (3) annually publicly report on their compliance.

President Trump and the Republican-majority Congress are expected to seek to roll back at least some aspects of Dodd-Frank. The repeal of the Conflict Minerals Rule is explicitly provided for in the Financial Choice Act, which was introduced in the House during the last term. However, at present, most of the Conflict Minerals Rule remains very much in effect and is likely to remain so for at least the current reporting period, which requires filings in respect of calendar 2016 to be made by May 31, 2017. In the meantime, the Securities and Exchange Commission’s April 2014 stay of the mandatory audit requirement under the Rule is expected to remain in effect for this year (see our Alert discussing the audit stay here).

The ultimate fate of the Conflict Minerals Rule is likely to turn on whether Congress decides to take a narrow or broad brush approach to Dodd-Frank repeal. However, even if the Rule is repealed, many large companies have indicated that they will continue to expect suppliers to trace the origin of the 3TG in their products, maintain compliance programs and responsibly source 3TG. These requirements will ripple through many supply chains in much the same way as if the Rule were to remain in effect.

Finally, NGOs continue to review and rank filings. This past year, one NGO survey ranked both medical device companies and drug manufacturers, the latter for the first time as a separate category. As is the case with other supply chain compliance and corporate social responsibility issues, larger consumer facing brands that are perceived as compliance laggards face the greatest risk of being targeted by NGOs and socially responsible investors.

**EU Conflict Minerals Regulation.** During November 2016, the EU Council, Commission and Parliament reached an informal final agreement on a conflict minerals regulation. The Regulation generally will require EU smelters and
refiners and direct importers of 3TG into the European Union to conduct due diligence using the OECD Guidance framework if they are sourcing from conflict-affected and high-risk areas anywhere in the world. For more information on the pending Regulation, see our Alert here.

The text of the final Regulation is expected to be released soon, after which it will be submitted for approval to the Council and the Parliament. The Regulation will take effect on January 1, 2021.

The Regulation generally will not impose compliance obligations on manufacturers or sellers of components or finished products. However, many larger “downstream undertakings” will expect their suppliers to make supply chain inquiries and source 3TG from conflict-free smelters and refiners. This will result in compliance obligations to meet commercial requirements, for a significant number of supply chain participants that are not subject to the Regulation. In addition, many larger downstream companies and the NGO community are expected to push for voluntary supply chain compliance prior to 2021.

**EU RoHS and REACH**

The continuing phase-in and expansion of RoHS (Restriction of Hazardous Substances) and REACH (Registration, Evaluation, Authorisation and Restriction of Chemicals) to new substances and product categories will require enhancements to supply chain compliance programs in 2017 and beyond.

**RoHS.** RoHS prohibits electrical and electronic equipment that contains enumerated toxic substances in specified concentrations from being placed on the EU market. RoHS also contains affirmative compliance requirements, such as requiring “CE” markings and declarations of conformity.

There currently are six restricted substances under RoHS, coupled with phase-ins for eleven product categories that run through July 2019 (many categories have already been fully or partially phased in). During mid-2015, four new substances – all phthalates – were added. Restrictions on the use of these substances generally will take effect during July 2019 and July 2021.

**REACH.** REACH is more broadly intended to protect human health and the environment from risks posed by chemicals. REACH contains procedures for collecting, assessing and reporting information to customers and the European Chemicals Agency on substances manufactured in or imported into the European Union. For some substances, REACH goes further, requiring authorization or restricting how the substances can be supplied or used.

There currently are approximately 170 substances of very high concern (SVHCs) on the REACH candidate list, and the list continues to grow. In addition, pursuant to a decision of the EU Court of Justice in September 2015, the .1% weight to weight REACH reporting threshold must be applied at the individual article or component level, rather than at the finished good or complex product level, which in many cases greatly expands the requirement to drill down and report on SVHC content in products.

**About our Supply Chain Compliance Practice**

Ropes & Gray has a leading supply chain compliance and corporate social responsibility practice. We advise clients across a broad range of regulations, commodities and geographies, and our clients include leading public and private companies and trade groups from every major industry.

With on-the-ground expertise in the United States, Europe and Asia, we are able to take a holistic, global approach to supply chain compliance and CSR, to help clients efficiently and effectively structure and implement their supply chain compliance and CSR programs and mitigate risk.
For further information on our supply chain compliance practice or if you would like to learn more about the topics in this Alert, please contact your usual Ropes & Gray attorney or contact us here.

**Ropes & Gray Supply Chain Compliance and CSR Mailing List**

[Click here](#) to join the Ropes & Gray Supply Chain Compliance and CSR mailing list to receive Alerts, articles and program announcements relating to supply chain compliance, or to sign up for other Ropes & Gray mailing lists.

**Ropes & Gray Supply Chain Compliance and Corporate Social Responsibility Resource Center**

As part of our commitment to excellence in this area, we have developed the Resource Center as a free educational tool for our clients, friends and other stakeholders. The Resource Center is the most extensive complimentary collection of supply chain compliance resources and is frequently updated to reflect new developments in this dynamic area. [Click here](#) to go to the Resource Center.
Case Closed! – The Conflict Minerals Rule Litigation Is Over, but the Drama Continues

After 1,627 days and enough law firm memos to deforest a small country, the litigation relating to the Conflict Minerals Rule came to an end yesterday. In this Alert, we discuss what this means for calendar year 2016 compliance, as well as the many other moving pieces relating to the Rule.

The Court’s Final Judgment

Yesterday, Judge Ketanji Brown Jackson, a District Court Judge in the District of Columbia, entered a final judgment in the Conflict Minerals Rule case. In a short three paragraph opinion, the District Court (1) declared that Section 1502 of Dodd-Frank, Rule 13p-1 thereunder and Form SD violate the First Amendment to the extent that the statute and the rule require companies to report to the SEC and state on their websites that any of their products “have not been found to be ‘DRC conflict free,’” (2) held unlawful and set aside the Rule to the extent that it requires companies to report to the SEC and state on their websites that any of their products “have not been found to be ‘DRC conflict free’” and (3) remands to the SEC, to take action in furtherance of the Court’s decision.

Judge Jackson’s decision was expected. On March 10th, the parties submitted a Joint Status Report requesting that the Court enter a final judgment in accordance with the earlier decisions in the case by the Court of Appeals. The appellate court decision is discussed in our earlier Alert available here.

But the Uncertainty Continues

Although the litigation has come to a close, the uncertainty surrounding the Conflict Minerals Rule continues:

- The SEC is expected to publish a new Statement that supersedes its April 29, 2014 Statement, which was put out in response to the Court of Appeals’ April 14, 2014 decision. In its 2014 Statement, the SEC indicated that companies are not required to identify products as “DRC conflict free,” having “not been found to be ‘DRC conflict free’” or “DRC conflict undeterminable.” In addition, the Statement indicated that, pending further action, an independent private sector audit will not be required unless a company voluntarily elects to describe a product as “DRC conflict free” in its Conflict Minerals Report. The April 2014 Statement is discussed in our Alert available here.

  The $64,000 question is whether the SEC will reinstate the mandatory audit requirement contemplated by the Conflict Minerals Rule. We think that the chances of this occurring for the upcoming calendar 2016 filing are nil. Looking further out, for various reasons, we think that the mandatory audit requirement is unlikely to be reinstated, but it is not impossible if the Rule survives.

- On January 31st, SEC Acting Chairman Piwowar published Statements directing the SEC staff to consider whether the SEC’s 2014 guidance is still appropriate and whether any additional relief is appropriate in the interim, and opening up a comment period on the Rule, which closed during the middle of March. Putting aside form letters, the SEC received approximately 300 comment letters, both supporting and against the Rule, as well as letters taking the middle ground by advocating for modifications to the Rule.
Last week, four Democrats on the Senate Banking Committee sent a letter to the SEC’s Inspector General asking him to conduct an investigation into whether this and other unrelated actions taken by Acting Chairman Piwowar were legally permissible.

Whether and when the SEC might modify the Rule in response to comments received and the lessons learned from four years of compliance by companies, and whether the letter to the IG might temper its appetite to do so, remain open questions.

- In early February, a draft of a purported Presidential Memorandum that would suspend the Conflict Minerals Rule began to circulate. Under Section 1502 of Dodd-Frank, the SEC is required to revise or temporarily waive the requirements of the Rule if the President transmits to the SEC a determination that doing so is in the national security interest of the United States and the President includes the reasons therefor. Under Section 1502, the revision or waiver can last for up to two years.

The draft Memorandum contemplates a two-year waiver. The draft Memorandum also directs the Secretaries of State and Treasury to propose an alternative plan to address problems in the DRC region that takes a targeted approach focused on breaking the link between commodities and armed groups in the region. Thus far, the White House has not commented on the draft Memorandum in circulation.

For more information on the draft Memorandum, please see the webinar hosted by Assent Compliance in which we participated, which is available here.

- On March 27th, the State Department announced that it, along with other agencies and departments, is seeking input from stakeholders to inform recommendations of how best to support responsible sourcing of 3TG. The Department will consider requests and comments received or postmarked by April 28th.
- The Financial Choice Act introduced during 2016 contemplated the repeal of Section 1502 of Dodd-Frank. The chances are high that repeal of Section 1502 will be sought in successor legislation.
- Finally, Jay Clayton, the President’s nominee for SEC Chairman, is moving closer to being seated. The Senate Banking Committee is scheduled to vote today, after which he will move to confirmation by the full Senate. As SEC Chairman, he will drive many aspects of the SEC’s agenda, including conflict minerals regulation.

Compliance in the Near Term

So where does all of the above leave companies? For the time being, the status quo is maintained. Except as modified by the SEC’s April 2014 Statement, the Conflict Minerals Rule continues in effect and calendar year 2016 filings continue to be due on May 31st.

But, stay tuned. The roller coaster ride continues.

Meanwhile, in the EU

In other news, yesterday, the European Council voted to approve the pending EU conflict minerals regulation. The regulation was previously approved by the EU Parliament and follows on the November 22, 2016 political agreement reached by the Parliament and the Council.

The EU conflict minerals regulation, which places mandatory obligations on importers of 3TG but not product manufacturers and sellers, takes effect on January 1, 2021. Please see our earlier Alert for a summary of the EU regulation. More extensive commentary from Ropes & Gray on the final regulation will be forthcoming.
About Our Supply Chain Compliance and CSR Practice

Ropes & Gray has a leading supply chain compliance and corporate social responsibility practice. We advise clients across a broad range of regulations, commodities and geographies, and our clients include leading public and private companies and trade groups from every major industry.

With on-the-ground expertise in the United States, Europe and Asia, we are able to take a holistic, global approach to supply chain compliance and CSR, to help clients efficiently and effectively structure and implement their supply chain compliance and CSR programs and mitigate risk.

For further information on our supply chain compliance and CSR practice or if you would like to learn more about the topics in this Alert, please contact your usual Ropes & Gray attorney or contact us here.

Ropes & Gray Supply Chain Compliance and CSR Mailing List

Click here to join the Ropes & Gray Supply Chain Compliance and CSR mailing list to receive Alerts, articles and program announcements relating to supply chain compliance and corporate social responsibility, or to sign up for other Ropes & Gray mailing lists.

Ropes & Gray Supply Chain Compliance and Corporate Social Responsibility Resource Center

As part of our commitment to excellence in this area, we have developed the Resource Center as a free educational tool for our clients, friends and other stakeholders. The Resource Center is the most extensive complimentary collection of supply chain compliance resources and is frequently updated to reflect new developments in this dynamic area. Click here to go to the Resource Center.
SEC Issues Updated Statement on Conflict Minerals Rule

On Friday afternoon, the SEC’s Division of Corporation Finance issued an Updated Statement on the Conflict Minerals Rule (the “Rule”). An updated Statement was widely anticipated. Earlier in the week, on April 3rd, the U.S. District Court for the District of Columbia entered its final judgment in the case and remanded to the SEC. This Alert discusses the Statement and other related developments, as well as short-term compliance considerations.

The District Court Judgment – A Recap

In its final judgment, the District Court (1) declared that Section 1502 of Dodd-Frank, Rule 13p-1 thereunder and Form SD violate the First Amendment to the extent that the statute and the rule require companies to report to the SEC and state on their websites that any of their products “have not been found to be ‘DRC conflict free,’” (2) held unlawful and set aside the Rule to the extent that it requires companies to report to the SEC and state on their websites that any of their products “have not been found to be ‘DRC conflict free’” and (3) remands to the SEC, to take action in furtherance of the Court’s decision. The judgment is discussed in our earlier Alert.

The Division of Corporation Finance's Statement

According to the April 7th Statement of the SEC’s Division of Corporation Finance, the Court’s remand has presented significant issues for the SEC to address. In light of the uncertainty regarding how the SEC will resolve those issues and related issues raised by commenters in the recent open comment period on the Rule, the Division has indicated that it will not recommend enforcement action to the Commission if registrants, including those that are subject to paragraph (c) of Item 1.01 of Form SD, only file disclosure under the provisions of paragraphs (a) and (b) of Item 1.01 of Form SD.

Paragraph (a) of Item 1.01 requires a reasonable country of origin inquiry (“RCOI”) if conflict minerals are necessary to the functionality or production of a product manufactured or contracted to be manufactured by a registrant. Paragraph (b) provides that, if, based on its RCOI, the registrant determines that its necessary conflict minerals did not originate in the DRC region or came from recycled or scrap sources, it has no reason to believe that its necessary conflict minerals may have originated in the DRC region, or it reasonably believes that its necessary conflict minerals did come from recycled or scrap sources, it must, in the body of its Form SD, disclose its determination and briefly describe the RCOI it undertook and the results of the inquiry it performed. For those registrants that are not able to stop at the RCOI, paragraph (c) of Item 1.01 generally requires the registrant to exercise due diligence and file a Conflict Minerals Report exhibit to its Form SD that contains enhanced disclosure on the registrant’s due diligence measures, its in-scope products and the processing facilities and countries of origin of the necessary conflict minerals.

The Division’s Statement indicates that it is subject to any further action that may be taken by the SEC, expresses the Division’s position on enforcement action only and does not express any legal conclusion on the Conflict Minerals Rule.

Acting Chairman Piwowar’s Statement

Also on Friday, SEC Acting Chairman Piwowar published a separate Statement. In his Statement, he indicated that he has instructed the SEC staff to begin work on a recommendation for future SEC action and that, in preparing its
recommendation, the Staff will consider, among other things, the public comments received in response to the January 31st request for comment on the Rule. Acting Chairman Piwowar, who has made it well known that he is opposed to the Rule, further indicated in his Statement that “[t]he primary function of the extensive and costly requirements for due diligence on the source and chain of custody of conflict minerals set forth in paragraph (c) of Item 1.01 of Form SD is to enable companies to make the disclosure found to be unconstitutional.” and that “[i]n light of the foregoing regulatory uncertainties, until these issues are resolved, it is difficult to conceive of a circumstance that would counsel in favor of enforcing Item 1.01(c) of Form SD.”

**Early Reactions to the Statements**

News sources have reported that SEC Commissioner Kara Stein, a Democratic Commissioner and currently the only other seated SEC Commissioner, has taken exception to Acting Chairman Piwowar’s action. She has accused him of acting beyond his authority to engage in de facto rulemaking.

As of Sunday afternoon when this Alert was prepared, the NGOs focused on this issue have not published statements, but we expect those to be forthcoming this week. We also would not be surprised to see another shot across the bow from Democrats on the Senate Banking Committee. On March 29th, four Democrats on the Senate Banking Committee sent a letter to the SEC’s Inspector General asking him to conduct an investigation into whether Acting Chairman Piwowar’s January 31st Statement opening up a comment period on the Rule and other unrelated actions taken by Acting Chairman Piwowar were legally permissible.

**Near Term Steps for Registrants**

The Statements will have little impact on the calendar year 2016 traceability process at most registrants. In most cases, that process has been completed or is close to completion. And, in any event, there is significant overlap between the RCOI and due diligence processes.

For most registrants, the most immediate considerations will be how much to say in the calendar year 2016 Form SD and whether to include a separate Conflict Minerals Report exhibit. As a result of the Division of Corporation Finance’s Statement, we expect that there will be more variation in disclosure this year relative to calendar year 2015 reporting. Among the factors that registrants will be considering in crafting their disclosure are NGO and socially responsible investor pressure around responsible minerals sourcing and disclosure rankings, messaging to commercial customers and consumers, internal corporate social responsibility values and their best guestimate as to where the Rule and market practice will be heading over the next year. Some of the factors that will determine the ultimate outcome of the Rule are discussed in this Alert. In that Alert, we indicated that the drama around the Rule would continue, and, for now, it shows no sign of abating.

**About Our Supply Chain Compliance and CSR Practice**

Ropes & Gray has a leading supply chain compliance and corporate social responsibility practice. We advise clients across a broad range of regulations, commodities and geographies, and our clients include leading public and private companies and trade groups from every major industry.

With on-the-ground expertise in the United States, Europe and Asia, we are able to take a holistic, global approach to supply chain compliance and CSR, to help clients efficiently and effectively structure and implement their supply chain compliance and CSR programs and mitigate risk.

For further information on our supply chain compliance and CSR practice, or if you would like to learn more about the topics in this Alert, please contact your usual Ropes & Gray attorney or contact us [here](mailto:here).
Ropes & Gray Supply Chain Compliance and CSR Mailing List

Click here to join the Ropes & Gray Supply Chain Compliance and CSR mailing list to receive Alerts, articles and program announcements relating to supply chain compliance and corporate social responsibility, or to sign up for other Ropes & Gray mailing lists.

Ropes & Gray Supply Chain Compliance and Corporate Social Responsibility Resource Center

As part of our commitment to excellence in this area, we have developed the Resource Center as a free educational tool for our clients, friends and other stakeholders. The Resource Center is the most extensive complimentary collection of supply chain compliance resources and is frequently updated to reflect new developments in this dynamic area. Click here to go to the Resource Center.
Evaluating FCPA Pilot Program: The Data, The Trends

This article by government enforcement partners Ryan Rohlfsen and Kim Nemirow and associates Dante Roldan and Sarah Kimmer was published by Law360 on April 14, 2017.

April 5 marked the one-year anniversary of the "Foreign Corrupt Practices Act Enforcement Plan and Guidance."1 Announced by the U.S. Department of Justice, Criminal Division's Fraud Section, the guidance outlined three important steps employed by the DOJ in combating FCPA violations: increased FCPA enforcement resources, international cooperation and, most notably, the launching of the FCPA enforcement pilot program.

The pilot program formalized the DOJ’s practice of rewarding corporate cooperation and remediation with penalty reductions beyond what was historically available under the sentencing guidelines. Fashioned as both a carrot and a stick, the pilot program incentivizes companies who self-disclose potential violations to the DOJ and penalizes those who do not. Specifically, under the pilot program, a cooperating company could receive only up to a 25 percent reduction or “discount” from the bottom of the sentencing guidelines fine range if it did not disclose the wrongdoing whereas it could earn a possible declination or up to a 50 percent discount if it promptly self-disclosed the conduct.

The pilot program was initially designed to be a one-year test, during which time the Fraud Section would determine whether the program would be extended in duration or to modify its policies. On March 10, 2017, the DOJ announced that the pilot program would remain in place after its April 5, 2017, expiration while the DOJ continues to evaluate its efficacy.2

This article will discuss patterns and key takeaways from the pilot program’s first year. Notably, the DOJ has resolved 18 FCPA cases over the last 12 months, a significant increase compared to the seven resolutions from the prior 12-month period. As indicated in the scatter plot following the article, a close review of the 18 matters provides substantial data from which to analyze the pilot program’s short-term impact.

Year in Review

Since the announcement of the pilot program, the DOJ has resolved 18 FCPA cases. Geographically, there continues to be a concentration of cases with conduct originating in China (eight of 18). There is also growing number of actions related to activity in Latin America — six this year, compared to four in the preceding year. The rise in Latin American actions is likely the result of local enforcement agencies’ increased focus on anti-corruption in the wake of the Petrobras scandal, among other high-profile prosecutions.

Over the last year, seven companies resolved self-reported misconduct, and five received the pilot program’s maximum reward — a declination. This is once again an uptick from the prior year, when the DOJ issued

declinations in only two cases. The two other companies that self-disclosed under the pilot program, but did not receive declinations, General Cable Corp. and Analogic Corp., received a 50 percent and 30 percent discount, respectively. Further, no company that self-reported was required to engage a corporate compliance monitor. All seven self-disclosing companies, however, were required to disgorge profits per the pilot program’s requirements.

Interestingly, the DOJ overwhelmingly imposed monitorships with both nonprosecution agreements and deferred prosecution agreements resolutions. Nine of the 11 NPA and DPA resolutions required the company to appoint a monitor. From this group, only Rolls Royce PLC and JPMorgan were spared the imposition of a monitor.

**Key Trends Under the Pilot Program**

The DOJ’s application of the pilot program over the last year has yielded some degree of consistency. Three trends — cooperation, monitorships and self-disclosure — have emerged as key considerations for companies investigating potential misconduct.

**Cooperation Is Key**

The pilot program allows for as much as a 25 percent reduction in fines for companies that cooperate with a DOJ investigation, but did not self-report the misconduct. Of the 11 settlements involving companies that did not self-report, nine received a discount of 25 percent or less. Five of the seven companies that self-reported and fully cooperated, received declinations from the DOJ and were required to pay disgorgement — but no fines or penalties — to resolve their FCPA misconduct. The prior year’s resolutions were arguably not as consistent on this point.³

Regardless of whether a company self-reports misconduct, the level of cooperation may also impact the potential discount. Companies that received less than the maximum discount also did not receive full cooperation credit from the DOJ. For example, Analogic did not initially disclose all relevant facts to the DOJ. As a result, it similarly received a 30 percent discount, instead of the full 50 percent available to self-disclosing companies under the pilot program.⁴ Similarly, according to the DPA, Embraer.

SA fully cooperated with the DOJ’s investigation but only partially remediated. The DPA notes that Embraer did not terminate a senior executive with knowledge of the conduct described in the DPA, which was a factor that the DOJ considered when determining that Embraer would receive a 20 percent discount in lieu of a potential 25 percent discount for companies who had fully cooperated and remediated.⁵ For Braskem SA, Teva Pharmaceuticals Industries Ltd. and Och-Ziff Capital Management Group LLC, delays during the early stages of the investigations, led to decreased discounts of 15 percent, 20 percent, and 20 percent, respectively, instead of the maximum 25 percent discount available to each company.

---

³ In 2015, the DOJ declined to take action in two cases, Petro Tiger and SAP, but only Petro Tiger self-disclosed its misconduct. In the remaining five cases, the fine discounts ranged from 0 percent to 45 percent, with no two companies receiving the same discount.
Monitorships Are a Very Real Possibility

Recent resolutions confirm that self-reporting companies have been far less likely to receive a monitor. Comparatively, those companies that do not self-disclose have been increasingly subject to review by a monitor. The data over the last year bears this out — nine of the companies that did not self-report were required to appoint a monitor, compared to two self-reporting companies where a monitor was not required.

The DOJ’s decision to impose a monitor generally turns on whether the company has “implemented an effective compliance program.” However, non-self-reporting companies that received full cooperation credit and implemented (according to the resolution papers) strong compliance enhancements, still overwhelmingly received monitorships. This trend is also noteworthy because the imposition of a monitorship may represent a significant expense for companies on top of any fines, and may exceed the value of a discount off the sentencing guidelines.

As noted above, although they did not self-report, neither JPMorgan nor Rolls Royce received a monitor. The DOJ determined that “an independent compliance monitor was unnecessary” for JPMorgan based on the “state of [the company’s] compliance program” and its agreement to provide periodic reports to the DOJ and the U.S. Attorney’s Office for the Eastern District of New York. In the case of Rolls Royce, the U.K.-based company entered into $800 million global resolution with authorities in the United Kingdom, United States and Brazil. Of that amount, the U.K. received $605 million, the U.S. $170 million, and Brazil $25 million. Based on the size of the U.K. portion of the settlement, compared to those with the U.S. and Brazil, it is possible that the DOJ deferred to the U.K. regarding such issues as to whether to impose a Monitor.

DOJ Further Incentivizes Self-Disclosure

Over the last year, the majority of self-reporting companies (five of seven) received declinations. The remaining companies, Analogic and General Cable, received significant discounts and were not required to engage a monitor. Companies should consider these results when making a disclosure decision.

The terms of the DOJ’s settlement with Analogic, despite the company’s incomplete self-disclosure, signals the value the government places on self-reporting. While Analogic self-reported a scheme whereby a subsidiary funneled millions of dollars to third parties, including government officials in Russia, it failed to initially disclose all relevant facts. Nevertheless, the DOJ credited Analogic for its self-disclosure and cooperation during the investigation. As result, Analogic settled upon a $3.4 million fine — a 30 percent discount — and was not required to engage a monitor.

Limitations on Declinations

Despite the penalty consistency of the first year, the full impact of the pilot program remains to be seen. While the DOJ has resolved cases under the pilot program’s guidance, these matters were apparently reported prior to its launch. We expect that cases handled entirely within the pilot program’s framework will be resolved later in 2017 and may provide more clarity, particularly with respect to the use of declinations.

7 JPMorgan NPA, supra note 6.
8 BK Medical NPA, supra note 4.
Contrary to the five self-disclosed cases that received declinations, General Cable’s resolution provides support for the notion that the size and scope of self-reported conduct will inform whether a company receives a declination. General Cable self-reported a scheme whereby foreign subsidiaries used third-party agents and distributors to make corrupt payments to foreign officials in Angola, Bangladesh, Indonesia, Thailand and China to obtain business. Disgorgement — typically calculated from the profits attributable to the misconduct — is at least one indicia of the size of a company’s misconduct. In addition to a three-year NPA with the DOJ, General Cable disgorged $55 million in a separate resolution with the U.S. Securities and Exchange Commission.

General Cable’s $55 million disgorgement payment was almost six times the highest amount paid by the five self-reporting companies that received declinations. Indeed, three of the five companies receiving declinations paid disgorgement that did not exceed $700,000. The size of General Cable’s disgorgement sheds light on the existence of an upper limit to the types of self-reported schemes that will receive declinations.

**Looking Forward**

While the pilot program continues, its future is by no means set in stone. Instead, the DOJ will continue to evaluate the pilot program’s “utility and efficacy” to determine “whether to extend it, and what revisions, if any” should be made.9

Importantly, the pilot program was announced also as an initiative to cooperate with international regulators. In fact, the DOJ has credited foreign authorities with providing valuable assistance in nearly ever resolution over the last year. Furthermore, a number of foreign jurisdictions have ramped up anti-corruption investigations and enhanced international cooperation. For example, prosecutors from 10 Latin American countries (Brazil, Argentina, Chile, Colombia, Ecuador, Mexico, Peru, the Dominican Republic, Venezuela and Panama) and one European country, Portugal, recently announced that they will form a task force to share evidence in the investigation of bribes paid by Odebrecht SA.10 The goal of the task force is to speed up the exchange of information between countries to avoid “bureaucratic hurdles” encountered when assessing penalties.11

In summary, the DOJ’s FCPA enforcement does not appear to be on the decline. Further anti-corruption developments abroad will only serve to increase pressure on the DOJ to strengthen its FCPA efforts.

---

9 Blanco Speaks at the American Bar Association National Institute on White Collar Crime, supra note 2.
11 Id.
This alert should not be construed as legal advice or a legal opinion on any specific facts or circumstances. This alert is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. The contents are intended for general informational purposes only, and you are urged to consult your attorney concerning any particular situation and any specific legal question you may have. © 2017 Ropes & Gray LLP

*The government declined to take action against Nortek, Akamai, Johnson Controls, HMT, and NCH.*
February 1, 2017

Privacy Implications of President Trump’s Immigration Order

On Wednesday, January 25, President Donald J. Trump directed federal agencies, “to the extent consistent with applicable law,” to ensure that “their privacy policies exclude persons who are not U.S. citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information.” That directive, Section 14 of an Executive Order that expands enforcement of U.S. immigration laws, is a departure from how the federal government previously has treated personally identifiable information (“PII”) of those who are not U.S. citizens or lawful permanent residents (“non-U.S. persons”) in many contexts, including the processing of visas and immigration records.

The Privacy Act of 1974 requires federal agencies to meet specific minimum privacy standards with respect to PII in databases they maintain. The Privacy Act is frequently recognized for promoting the Fair Information Practice Principles (“FIPPs”), which have become a widely accepted framework for evaluating and considering systems, processes or programs that impact individual privacy. The FIPPs have served as a model for the privacy laws of many U.S. states, foreign countries and international organizations.1

Although the Privacy Act only requires that federal agencies apply minimum privacy standards to the PII of U.S. citizens and lawful permanent residents,2 many agencies historically have applied the same standards to the PII of non-U.S. persons as well.3 In addition, the Judicial Redress Act of 20154 gives the Attorney General discretion to extend the rights and remedies of the Privacy Act to citizens of specific regional economic integration organizations and foreign countries to the extent they are so designated in the Federal Register. Pursuant to the Judicial Redress Act, outgoing Attorney General Loretta Lynch officially designated the EU and most EU member countries as “covered” countries whose citizens are afforded Privacy Act protections, effective February 1, 2017.5 As a result, the Privacy Act now covers the processing of personal data of EU citizens by federal agencies in the United States. Nothing in Section 14 changes this coverage, because the Executive Order does not trump the Judicial Redress Act or the Federal Register designations.

A. Initial Privacy Impact

In order to comply with Section 14, federal agencies will need to revise their privacy policies to exclude non-U.S. persons. In the short term, these changes primarily will impact non-U.S. persons who are citizens of countries outside of the EU, because any changes must be consistent with the Judicial Redress Act, which extends the protections of the Privacy Act to EU citizens based on the current Federal Register designations.

Pursuant to their revised privacy policies, however, agencies lawfully may ignore the FIPPs when processing the PII of non-U.S. persons who are citizens of countries outside of the EU. For example, agencies may disclose the PII of such non-U.S. persons without their consent to other agencies or third parties. While disclosures of this sort

---

3 See, e.g., Department of Homeland Security Privacy Policy Guidance Memorandum No. 2007-1 (2007) (“As a matter of DHS policy, any personally identifiable information (PII) that is collected, used, maintained, and/or disseminated in connection with a mixed system by DHS shall be treated as a System of Records subject to the Privacy Act regardless of whether the information pertains to a U.S. citizen, Legal Permanent Resident, visitor, or alien.”).
5 The designations will become effective simultaneously with the U.S.-EU Data Protection and Privacy Agreement (DPPA). Congress passed the Judicial Redress Act in order to implement the redress right provisions of the DPPA.
presumably include the Executive Order’s proposed publication of lists of crimes committed by aliens,\(^6\) the ability to share information freely appears to sweep more broadly. Agencies may no longer be able to:

- provide non-U.S. persons who are citizens of countries outside of the EU with access to PII concerning them that is maintained in agency databases;
- devote resources to ensure that PII of such persons is accurate, relevant, timely and complete; or
- consider requests from such persons that their records be amended.

As a result, non-U.S. persons from countries outside the EU may be unable to confirm that data held about them is correct, or request that mistakes in such data be corrected.

**B. Longer-Term Privacy Impact**

Although some European commentators have voiced concern that the Executive Order threatens the viability of the recently enacted EU-U.S. Privacy Shield framework for regulating transatlantic data transfers, the EU Commission reportedly indicated in an [emailed statement](#) that such concerns are unfounded. The Commission added that the U.S.-EU Data Protection and Privacy Agreement, which establishes a set of protections, including specific judicial redress rights, for PII exchanged between the United States and the EU for law enforcement purposes, also will remain in place.

Once confirmed, the new Attorney General will have some discretion under the Judicial Redress Act to remove the designations of the EU and most EU member countries as “covered” countries whose citizens are afforded Privacy Act protections. Nonetheless, the new Executive Order does not require such removal explicitly. Unless the European Commission decides to reconsider whether the privacy rights afforded EU citizens under the Judicial Redress Act adequately protect their PII, it is too soon to say whether the Executive Order specifically will impact the Privacy Shield status quo.

---

\(^6\) See Section 9(b) of the Executive Order.
The GDPR – Possible Impact on the Life Sciences and Healthcare Sectors

Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016, (the “GDPR”) came into force in May 2016 and introduced a number of changes to European data protection law. Such changes will impact many entities conducting business within the European Union (the “EU”); however, the implications for organizations operating in the life sciences and healthcare sectors are likely to be particularly far-reaching. Life sciences and healthcare-related businesses often collect and/or use large amounts of sensitive health-related data in respect of living individuals, such as patients and clinical trial subjects, so the new data protection requirements will be particularly relevant for them.

We set out below a summary of some of the more significant changes that are likely to impact stakeholders within these sectors.

Extra Territorial Effect

Previously, European data protection legislation only applied to organizations that collected and/or used personal data if such organizations were established within the EU, or if they were established outside the EU, but used equipment within the EU to process personal data (unless this was only for transit purposes).

The GDPR will continue to apply to organizations established within the EU which process personal data; however, organizations established outside the EU will now also be subject to the GDPR if such organizations process the personal data of EU-based individuals and either (i) offer goods or services to individuals within the EU; and/or (ii) monitor the behavior of data subjects within the EU. Any non-EU-based entities to which the GDPR applies will be obliged to appoint a representative within the EU to ensure that they comply with the requirements of the GDPR when processing the personal data of European citizens in the ways set out above.

This means that more non-EU-based organizations operating in the life sciences and healthcare sectors (for example, contract research organizations involved in clinical trials, providers of healthcare services and health insurance companies) are likely to be subject to the GDPR, going forward, than were subject to previous European data protection legislation.

Special Categories of Personal Data

The GDPR prohibits the processing of certain special categories of personal data (or “sensitive personal data”), subject to certain exceptions. The special categories of personal data include, among other things, genetic data and data concerning health.

“Genetic data” is defined by the GDPR for the first time. “Genetic data” includes personal data relating to the inherited or acquired genetic characteristics of a natural person that give unique information about the physiology or health of that natural person and that result, in particular, from an analysis of a biological sample from the natural person in question.
Although data concerning health was protected as a special category of data under the previous EU data protection legislation, the GDPR also defines “data concerning health” for the first time. “Data concerning health” includes personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about his or her health status.

Organizations operating in the life sciences and healthcare sectors that collect and/or use any data concerning health, genetic data, or other types of sensitive personal data will need to ensure that they fall within one of the exceptional circumstances set out in the GDPR when the prohibition on the processing of sensitive personal data is deemed not to apply. Among others, these include circumstances where:

i. the individual to whom the sensitive personal data relates has given his/her explicit consent to the processing for one or more specified and lawful purposes (unless such consent is prohibited by applicable EU or Member State law). Obtaining consent from individuals under the GDPR is discussed further below;

ii. the processing is necessary to protect the “vital interests” of the individual to whom the relevant data relate or another individual where the data subject is physically or legally incapable of giving consent (generally, this exception can only be relied on in “life or death” type situations);

iii. the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or Member State law or pursuant to contract with a health professional and subject to certain conditions and safeguards; and

iv. the processing is necessary for public interest reasons in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of EU or Member State law that provides for suitable and specific measures to safeguard the rights and freedoms of data subjects, in particular professional secrecy.

It should also be noted that Member States may maintain or introduce further conditions, including limitations, regarding the processing of genetic data or data concerning health, so organizations will need to be confirm whether any such additional restrictions exist in the relevant EU Member States where they process any such data.

Consent

Many organizations and businesses operating in the life sciences and healthcare sectors rely on obtaining the explicit consent of individuals to justify the collection and use of their sensitive personal health-related or genetic data (although this is not the only legal basis for processing of such data that can be relied on). The GDPR introduces a number of additional requirements that must be met to ensure that any consents that are obtained can be relied upon.

The GDPR introduces a new definition of “consent”. “Consent” is defined to mean any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or clear affirmative action, signifies agreement to the processing of personal data relating to him or her. Valid consent can be obtained in various ways (e.g., by requiring individuals to sign consent forms, or by clicking on an electronic “I consent” button).
If processing is based on consent, organizations must be able to show that individuals have agreed to the processing of their personal data. Furthermore, if consent is given in a written declaration that also relates to matters other than the consent, the consent request must be presented in a way that is clearly distinguishable from the other matters, intelligible, easily accessible and in clear and plain language in order to be valid.

The GDPR also makes clear the fact that individuals have the right to withdraw their consent to the processing of their personal information at any time (although this will not affect the lawfulness of any personal data processing that was carried out before consent was withdrawn). Individuals must also be informed that they have the right to withdraw their consent before consent is given and withdrawing consent must be as easy as giving consent.

The GDPR also provides that consent is unlikely to be deemed to be freely given where the performance of a contract, including the provision of a service, is made conditional on consent to the processing of personal data that is not necessary in order to perform the contract.

Life sciences and healthcare-related businesses that are subject to the GDPR should consider the procedures and wording that they use when obtaining consent from individuals, for example, informed consent forms used in connection with clinical trials or patient treatment. Informed consent forms that complied with the requirements of the previous EU legislation are unlikely to be adequate to comply with the consent requirements of the GDPR, so these should be updated as necessary to make sure that they are robust. Some commentators have observed that the GDPR’s consent requirements are likely to make valid consent difficult to obtain in practice, so it will be interesting to see whether data controllers continue to rely on individual consent or seek to rely on alternative justifications for their processing of personal and sensitive personal data.

**Anonymisation and Pseudonymisation**

Many life sciences and health sector businesses use coded data, particularly in the context of clinical trials. The issue of whether or not such data constitutes personal data and therefore whether or not European data protection legislation applies to it has long been a controversial topic.

The GDPR defines “pseudonymisation” for the first time. Essentially, pseudonymisation is defined to mean the processing of personal data in such a way that the personal data can no longer be attributed to a specific individual without using additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.

Among other things, the GDPR provides that data protection principles should apply to any information concerning an identified or identifiable individual. It also makes clear that personal data that has undergone pseudonymisation that could be attributed to an individual by the use of additional information should be considered to be information on an identifiable individual (in other words, pseudonymised personal data which allows re-identification of individuals will often be considered to be personal data).

The GDPR provides that, in order to decide whether an individual is identifiable, all the means reasonably likely to be used, either by the relevant data controller or a third party to identify the individual directly or indirectly, should be considered. In deciding whether means are reasonably likely to be used to identify an individual, various objective factors should be considered, for example, the costs of and amount of time required for identification, taking into account the technology available at the time the data is processed and technological developments.
Life sciences and health sector businesses will need to consider carefully whether individuals who are the subjects of any coded data that they collect and/or use would be deemed to be identifiable for the purposes of the GDPR. If so, then they will need to comply with the provisions of the GDPR in respect of such pseudonymised personal data. Certain commentators have observed that effective pseudonymisation of personal data that does not allow re-identification of individuals will be difficult to achieve in practice. Pending further guidance from European regulators on this point, it is probably safer to assume as a default position that any coded data constitutes personal data for the purposes of the GDPR and comply with the GDPR’s requirements in respect of such data.

**Data Protection Design and Default and Privacy Impact Assessments**

The GDPR introduces new formal requirements in respect of data protection by design and default principles. When deciding on a system for personal data processing and also when using that system to carry out such processing, data controllers must now implement appropriate technical and organizational measures, such as pseudonymisation, that implement data protection principles (for example, data minimisation) effectively and incorporate appropriate safeguards into the processing of personal data to meet the GDPR’s requirements and protect individuals’ rights. The state of the art, costs of implementation and the nature, scope, context and purposes of the intended personal data processing must be considered, together with the risks of varying likelihood and severity for individuals’ rights and freedoms that are raised by the processing.

Data controllers must also put in place appropriate technical and organizational measures to ensure that, by default, only personal data that is necessary for each specific purpose of the processing is processed and that by default personal data is not made accessible without the individual’s intervention to an indefinite number of people.

Life sciences and healthcare organizations will need to introduce appropriate policies and procedures to ensure that appropriate measures and safeguards are incorporated when introducing new personal data processing systems, products or processes and to ensure that data protection by design and default principles are respected.

The GDPR also formally requires data controllers to carry out privacy impact assessments in relation to any personal data processing that is likely to result in high risks to individuals’ rights and freedoms, particularly where the processing uses new technologies. Privacy impact assessments must be carried out, in particular, in a number of specified circumstances, including where personal data processing involves large scale processing of certain sensitive personal data, including genetic data and data concerning health. Privacy impact assessments should include various elements and, where appropriate, data controllers are obliged to seek the views of data subjects or their representatives on the intended processing (without prejudice to the protection of commercial or public interests or the security of the processing).

Life sciences and healthcare organizations should carry out privacy impact assessments in any circumstances when they are proposing to process large amounts of sensitive health-related data (e.g., when designing and running clinical trials and introducing new products and/or services for patients). Potentially, they may also have to seek the views of the relevant individuals or their representatives about their intended personal data processing in these circumstances, at least to some extent.

**Data Processors**

In addition to imposing new requirements on data controllers, the GDPR imposes various data protection obligations directly on data processors for the first time (data processors include any natural or legal person, public authority, agency or other body that processes personal data on behalf of a data controller). For example, the GDPR extends to
data processors the requirement to ensure an adequate level of protection for personal data that is transferred outside the European Economic Area. Similarly, data processors must put in place appropriate technical and organizational security measures to protect personal data to create and maintain certain records of their personal data processing activities (among other things).

Life sciences and healthcare organizations who are acting as data processors on behalf of data controllers (e.g. contract research organizations acting on behalf of clinical trial sponsors) will need to ensure that they comply with all relevant requirements of the GDPR, going forward.

**Group Actions**

The GDPR gives individuals the right for the first time to mandate not-for-profit bodies, organizations or associations, which have been properly constituted under the law of an EU Member State, that have statutory objectives in the public interest and which are active in protecting individuals’ rights and freedoms regarding protection of their personal data, to take various actions on their behalf. Such bodies, organizations and associations may lodge complaints on the relevant individuals’ behalf, exercise certain rights to obtain effective judicial remedies against data protection regulators and data controllers and processors and receive compensation on the individuals’ behalf in certain circumstances.

The GDPR thus increases the possibility of “group action” style data protection claims within Europe. Such claims, which may increase the frequency and costs of data protection-related proceedings, could be especially relevant for life sciences and healthcare-related organizations that infringe individuals’ privacy rights, given the large amounts of sensitive health-related personal data that such organizations typically collect and use.

**Penalties**

The GDPR considerably increases the sanctions and penalties that can be imposed on organizations that breach its requirements. In particular, the maximum monetary penalties that can be imposed by European data protection regulators for serious breaches have been substantially increased to up to: (i) €20,000,000; or (ii) 4% of an undertaking’s global annual turnover, whichever is the greater.

Clearly, for life sciences and healthcare sector organizations that handle significant amounts of sensitive personal health related data, the imposition of such increased monetary penalties in the event of a serious breach could be highly significant, so ensuring that a robust data protection compliance program is in place will be critical.

**Summary of Significant Issues**

A checklist of significant issues that life sciences and healthcare sector organizations need to consider is set out below:

- Does the GDPR apply to your organization, even if it is based outside the EU?
- Has your organization established a robust data protection compliance program to ensure compliance with the GDPR?
- Has your organization established a valid legal basis for processing personal data, particularly data concerning health, genetic data and any other relevant special categories of personal data?
• Has your organization updated its procedures, forms and wording for obtaining individual consents to ensure compliance with the GDPR?

• Does your organization use pseudonymised or “coded” data from which living individuals can be re-identified? If so, does your organization comply with the GDPR’s requirements in respect of it?

• Has your organization implemented appropriate policies and procedures to ensure that data protection by design and default principles are respected?

• Has your organization implemented appropriate policies and procedures to ensure that data protection impact assessments are carried out where required?

• If your organization acts as a data processor in any circumstances, is it able to comply with its new obligations under the GDPR?

Conclusion

Although officially in force, the GDPR will not be enforced by European regulators until 28th May 2018. The matters discussed above highlight some of the issues that are likely to impact life sciences and healthcare-related organizations; however, there are also other, more general, issues raised by the GDPR that such organizations will need to consider.

Life sciences and healthcare-related businesses should take steps now to ensure that they are able to comply with the new requirements of the GDPR. This should help such organizations to build and maintain the trust and confidence of their customers, business partners, patients and other individuals whose personal data they collect and process and avoid breaches of relevant data protection rules. Organizations that are prepared for the GDPR are also more likely to avoid enforcement action by European regulators, legal action from data subjects, significant monetary penalties and the attendant reputational damage and negative publicity that can result.
March 3, 2017

Cookies Crumble? The draft EU Regulation on Privacy and Electronic Communications

Background

The European Commission recently published a proposed Regulation on Privacy and Electronic Communications (the “Regulation”). The Regulation aims to update and broaden the scope of current rules under the ePrivacy Directive (2002/58/EC) on confidentiality of electronic communications as well as align the rules for electronic communications, cookie usage and direct marketing with the forthcoming General Data Protection Regulation (“GDPR”).

In line with the GDPR, penalties for infringement may be severe, with fines for infringement of the cookies and unsolicited communication rules potentially amounting to the greater of €10 million or up to 2% of the worldwide annual revenue. Infringements of the rules relating to confidentiality of content and metadata may be higher, with fines capped at the greater of €20 million or up to 4% of the worldwide annual revenue.

Though the new Regulation is planned to come into effect at the same time as the GDPR on 25 May 2018, it must first be formally approved by both the Parliament and the Council on a relatively ambitious timetable before it becomes law. Ultimately, the Commission hopes that the proposed Regulation will increase the protection of people’s private lives and open up opportunities for new businesses.

Scope of the Proposed Regulation

The Regulation covers almost all businesses that operate in Europe but, like the GDPR, also extends to businesses outside the EU if they provide services to users in the EU (including where such services are offered free of charge).

The Regulation applies to the processing of communications data carried out in connection with electronic communications services and to information related to end users’ terminal equipment. The Regulation proposes extending coverage from telecoms companies and ISPs to also include providers of over-the-top (“OTT”) services, including popular instant messaging applications. It further covers anyone using cookies or similar tracking technologies as well as anyone engaging in electronic marketing, whether or not they are providing an electronic communications service.

The Regulation does not apply to electronic communications services that are not publicly available. It also is inapplicable to government authorities engaged in detecting crime or otherwise protecting public safety.

Electronic Communications Data

The Regulation distinguishes between two types of electronic communications data: electronic communications content and electronic communications metadata. Content refers to the actual information exchanged in an electronic communication, including text, voice, videos, images and sound, including, for example, a picture or video sent using instant messaging. Metadata refers to data processed by a network for the purposes of transmitting content, including information relating to the source and destination of a communication; the location, date, and duration of a communication; and the method of communication. For instance, data identifying that an instant message was sent at a specified time is metadata.

Many of the rules in the regulation require consent. Consent must be “freely given, specific, informed and unambiguous,” which is the same standard as the GDPR. Consent can be expressed by a statement or clear
affirmative action. This allows consent to be expressed by using the settings of an application, which simplifies the acceptance or refusal process for users.

Confidentiality

Under the Regulation, both electronic communications content and metadata must be kept confidential and must not be interfered with. However, the Regulation permits a limited number of exceptions to this basic rule in the following circumstances:

- Both content and metadata may be processed in order to (1) transmit the communication; (2) maintain or restore security; or (3) detect technical faults or errors in the transmission of the communication.

- Metadata may also be processed if (1) it is necessary to meet mandatory EU quality of service requirements; (2) it is necessary for billing; (3) it is necessary for detecting or stopping fraud or abuse; or (4) the end user consents to the processing for a specified purpose which could not be carried out using anonymised data.

- Content may also be processed if (1) for the sole purpose of providing a specific service, if the service cannot be provided without such processing and provided the end user has consented to the processing; or (2) the end user consents to the processing for a specified purpose which could not be carried out using anonymised data and the provider consults the GDPR’s supervisory authority.

Data Erasure

Electronic communications service providers must either erase or anonymise content after its receipt by the intended recipient. Metadata must similarly be erased or anonymised when it is no longer needed for transmitting the communication. The same exceptions of confidentiality listed above also apply to erasure of data. Metadata may be further retained until the end of a period in which a bill or payment may be lawfully challenged under national law.

Cookies and Terminal Equipment

The Regulation prohibits the use of cookies (and similar tracking technologies, such as hidden identifiers and device fingerprinting) unless (1) it is necessary for the sole purpose of transmitting the communication; (2) the end user has consented; (3) it is necessary for providing an information society service (e.g., to add items to an online shopping basket) requested by the end user; or (4) it is necessary for web audience measuring if carried out by the information society service requested by the end user. No consent is needed for first-party cookies used by a website to carry out web audience measuring.

In addition, if cookies are used, the Regulation prohibits collecting device information unless (1) it is done only to establish a connection; or (2) users are notified how the data will be collected, the purposes for which it will be used; and certain other information.

All communications software (e.g., web browsers and other applications allowing the retrieval and presentation of information on the internet) must offer functionality to prevent the use of third-party cookies. Upon installation, the software must inform the end user about the privacy settings options. To continue with the installation, the end user must consent to one of the settings. For software already installed as of 25 May 2018, these requirements must be complied with by the first update of the software and no later than 25 August 2018.

Direct marketing

The rules in relation to electronic direct marketing are broadly equivalent to current legislation under the ePrivacy Directive – subject to limited exceptions, opt-in consent will still be required before businesses are permitted to send electronic direct marketing. However, notable changes include the widening of the scope of the application of the rules to cover all electronic communications services, which include communications sent through instant messaging applications and Bluetooth.
For telephone calls, however, Member states may permit the placing of direct, non-automated, voice-to-voice marketing calls, provided that the end user has not expressed an objection to receiving such communications. Those placing marketing calls must inform end users of the marketing nature of the communication and of their identity. They must also give the end user the chance to easily exercise his/her right to withdraw his/her consent.

**Comment**

The proposed scope of the Regulation is quite broad, encompassing almost all modern businesses and providers of electronic communications services. By replacing the current e-Privacy directive with a regulation, the Commission aims to provide a uniform set of rules that protect privacy for people and businesses.

The Regulation may allow for new business opportunities, as traditional telecoms operators will have more opportunities to use data and provide additional services once consent is given. The Commission also says that the rules on cookies have been simplified, for example by not requiring consent for cookies to simply monitor web traffic, although given the stricter consent requirements in respect of other cookies used, even with browser level consent controls, those cookie pop-ups look unlikely to disappear or even to crumble.
Aside from Brexit, the outlook in Europe is focused on harmony and unity, measures well reflected in the Digital Single Market initiative. As part of this initiative, the European Commission recently published a proposed Regulation on Privacy and Electronic Communications. The regulation is aimed at creating a harmonious pan-European approach to e-privacy, replacing the current directive with a directly effective regulation designed to address the complexities of privacy in the age of social media and networked computing; to simplify and clarify the EU approach to the use of cookies and data harvesting; and to align e-privacy with the data protection principles enshrined in the General Data Protection Regulation, and the EU Charter of Fundamental Rights. Ultimately, the commission hopes that the proposed regulation will increase the protection of individuals’ private lives, open up opportunities for new businesses and simplify and streamline current rules on cookies, which should result in greater trust and security in the Digital Single Market.

Though the new regulation is planned to come into effect at the same time as the GDPR on May 25, 2018, it must first be formally approved by both the Parliament and the Council on a relatively ambitious timetable before it becomes law.

**Objectives of the E-Privacy Regulation**

There are three clear objectives underpinning the revision of the e-privacy regime in Europe. The first is a desire to protect both the privacy and confidentiality of electronic communications. This is to be achieved by controlling the ways in which network and service providers process electronic communications data, whether it be the content of electronic communications such as email or instant message, or whether it be metadata relating to the electronic communication itself, such as the place, time or identity of person sending the communication. The second objective is the protection of the individual’s right to privacy with regard to their activities when browsing the internet or using electronic devices. This is to be achieved by the regulation of tracking technology such as cookies. The final objective is the control of direct marketing communications to ensure that electronic communications are carried out efficiently without individuals being exposed to unsolicited commercial communications or spam.

**Scope of the Proposed Regulation**

The regulation applies to the processing of communications data carried out in connection with electronic communications services and to information related to end users’ terminal equipment. The regulation proposes extending coverage from telecoms companies and internet service providers to also include providers of over-the-top (“OTT”) services, including popular instant messaging applications. It further covers anyone using cookies or similar tracking technologies, as well as anyone engaging in electronic marketing, whether or not they are providing an electronic communications service.

The regulation does not apply to electronic communications services that are not publicly available. It also is inapplicable to government authorities engaged in detecting crime or otherwise protecting public safety.
The regulation covers almost all businesses that operate in Europe but, like the GDPR, also extends to businesses outside the EU if they provide services to users in the EU (including where such services are offered free of charge).

**Electronic Communications Data**

The regulation distinguishes between two types of electronic communications data: electronic communications content and electronic communications metadata. Content refers to the actual information exchanged in an electronic communication, including text, voice, videos, images and sound. For example, a picture or video sent using instant messaging is electronic communications content. Metadata refers to data processed by a network for the purposes of transmitting content, including information relating to the source and destination of a communication; the location, date, and duration of a communication; and the method of communication. For instance, data identifying that an instant message was sent at a specified time is metadata.

Many of the prohibitions set out in the regulation can be overcome where there is “end user consent.” “Consent” in this context is aligned with the GDPR and so must be “freely given, specific, informed and unambiguous.” Consent can be expressed by a statement or clear affirmative action. However, the regulation does add that, where feasible, consent may be expressed by using appropriate software settings of an application. This is intended to simplify the acceptance or refusal process for users as consent may be given by browser settings, provided that the software informs end users of privacy settings options and obliges the end user to consent to or select such privacy setting as part of the set up of the service. Software must also offer end users the option to prevent the placing of third party cookies.

What is not so clear is who the “end user” actually is for the purposes of the regulation. It is clear that an end user is a user of a service, though it is unclear whether the end user includes the sender, the recipient or both, in relation to any electronic communication.

**Confidentiality**

Under the regulation, both electronic communications content and metadata must be kept confidential and must not be interfered with. However, the regulation permits a limited number of exceptions to this basic rule in the following circumstances:

- Both content and metadata may be processed in order to: (1) transmit the communication; (2) maintain or restore security; or (3) detect technical faults or errors in the transmission of the communication.

- Metadata may also be processed if: (1) it is necessary to meet mandatory EU quality of service requirements; (2) it is necessary for billing; (3) it is necessary for detecting or stopping fraud or abuse; or (4) the end user consents to the processing for a specified purpose that could not be carried out using anonymized data.

- Content may also be processed: (1) for the sole purpose of providing a specific service, if the service cannot be provided without such processing and provided the end user has consented to the processing; or (2) if the end user consents to the processing for a specified purpose that could not be carried out using anonymized data and the provider consults its relevant supervisory authority for the purposes of the GDPR.
Data Erasure

Electronic communications service providers must either erase or anonymize content after its receipt by the intended recipient. Metadata must similarly be erased or anonymized when it is no longer needed for transmitting the communication. The same exceptions of confidentiality listed above also apply to erasure of data. Metadata may be further retained until the end of a period in which a bill or payment may be lawfully challenged under national law.

Cookies and Terminal Equipment

The regulation is technology neutral and thus covers PCs, laptop, smartphones and tablet devices. Across all devices it prohibits the use of cookies (and similar tracking technologies, such as hidden identifiers and device fingerprinting) unless: (1) it is necessary for the sole purpose of transmitting the communication; (2) the end user has consented; (3) it is necessary for providing an information society service (e.g., to add items to an online shopping basket) requested by the end user; or (4) it is necessary for web audience measuring if carried out by the information society service requested by the end user. No consent is needed for first-party cookies used by a website to carry out web audience measuring.

In addition, if cookies are used, the regulation prohibits collecting device information unless: (1) it is done only to establish a connection; or (2) users are notified how the data will be collected, the purposes for which it will be used; and certain other information.

All communications software (e.g., web browsers and other applications allowing the retrieval and presentation of information on the internet) must offer functionality to prevent the use of third-party cookies. Upon installation, the software must inform the end user about the privacy settings options. To continue with the installation, the end user must consent to one of the settings. For software already installed as of May 25, 2018, these requirements must be complied with by the first update of the software and no later than Aug. 25, 2018.

Direct Marketing

The rules in relation to electronic direct marketing are broadly equivalent to current legislation under the e-privacy directive. However, “direct marketing communication” is defined as any form of advertising whether written or oral, sent to one or more identified or identifiable end users of electronic communication services, which include communications sent through instant messaging applications and Bluetooth. Subject to limited soft opt-in exceptions as under the current regime, opt-in consent will still be required before businesses are permitted to send electronic direct marketing.

Comment

Is the scope too broad for effective enforcement?

The commission has flagged that reform is necessary to keep up with recent developments in IT-based services such as voice over internet protocol as well as the forthcoming GDPR. In particular, the commission has specifically named key OTT service providers, as needing to offer the same level of confidentiality as traditional telecommunication operators. The proposed scope of the regulation is consequently quite broad, encompassing almost all modern businesses and providers of electronic communications services — the likely result being that, if
adopted as drafted, the regulation will provide for a more level playing field among traditional, modern and future electronic communications service providers.

However, as with the GDPR, there still remain concerns over data protection authorities’ ability to successfully enforce the extraterritorial effect of the proposed new rules. European electronic communications service providers may therefore, quite legitimately, question whether the rules are actually stacked against them. It will remain to be seen what action, if any, European data protection authorities can and do take against entirely non-EU electronic communication service providers who fail to comply with the regulation’s requirements. If the rules are not, or cannot be, successfully enforced against such providers, then there is potential for the regulation to stifle business and innovation in the EU, as non-EU jurisdictions consequently become more attractive.

In line with the GDPR, penalties for infringement may be severe, with fines for infringement of the cookies and unsolicited communication rules potentially amounting to the greater of €10 million or up to 2 percent of the worldwide annual revenue. Infringements of the rules relating to confidentiality of content and metadata may be higher, with fines capped at the greater of €20 million or up to 4 percent of the worldwide annual revenue. How “proportionate and dissuasive” fines will be assessed for noncompliance for the proposed rules on cookies and similar technologies remains to be seen. Historically, this area has not been heavily enforced under the current regime, with very few examples of fines being levied for infringement (and even then the level of those fines has been generally low), which has been a major criticism of the current regime, with those who are playing by the rules understandably arguing that more needs to be done to ensure the rules are actually enforced. This may have an impact on the quantum assessment however, given that many European data protection authorities already have limited resources and will likely be concentrating on the GDPR enforcement. For this reason, it is difficult to see this situation changing substantially.

**Will a borderless Digital Single Market be hampered by national security protections?**

By replacing the current e-privacy directive with a regulation, the commission aims to provide a uniform set of rules that protect the privacy of people and businesses. However, as with the GDPR, specific national (i.e., member state) derogations may still apply.

In particular, similarly to the GDPR, the regulation fails to provide for specific provisions in relation to data retention, and individual member states are free (subject to compliance with EU law) to provide for their own retention rules and to limit the confidentiality of communications in order to safeguard “general public interests.” This general position is likely to conflict with the balance of necessity, legality and proportionality set out in recent rulings of the Court of Justice of the European Union. The result may be that although there is an overarching general compliance regime across the EU, communications service providers may still have to navigate a patchwork of different member-state national rules as far as data retention is concerned.

**Privacy for communications content and metadata?**

The regulation aims to guarantee the privacy of communications content and metadata, particularly since both can potentially reveal highly sensitive information and personal data about end users and other legal persons (e.g., businesses). It will be interesting to see how many OTT service providers attempt to obtain user consent for the retention and further processing of such data and how they do this — ultimately this could lead to new privacy banners and pop-ups when using OTT services. However, the regulation makes no provision for standardized
security measures to be applied, such as the requirement for end-to-end encryption and instead references the appropriate technical and organizational security measures of the GDPR. The obligation or lack of obligation to provide security is likely to be a point of tension in the EU Parliament as there are clear voices from politicians, law enforcement, privacy campaigners and consumer bodies supporting both sides of the argument.

**Will this be the end of the cookie consent pop-up?**

The commission believes that the rules on cookies have been simplified, for example by not requiring consent for strictly necessary cookies, nor first-party cookies used to simply monitor web traffic. Together with the ability to accept or refuse cookies through web browser settings, this is intended, at least partly, to remove or reduce the need for cookie banners and pop-ups. This is welcome news, but in reality, is likely to present further complications.

In particular, most websites use third-party and other nonstrictly necessary cookies, especially for the purposes of advertising on free-to-use internet services, in order to monetize internet content and services. As a result, such websites will likely prefer control of cookie consent at a website level, as opposed to relying on choices made by end users at a browser level. For instance, it would be reasonable to assume that if end users choose not to accept third-party cookies within their browser settings, websites using such cookies will therefore want, and need, to obtain end users’ consent to do so. This means that it is unlikely that cookie consent banners will disappear under the regulation, which somewhat defeats the purpose of the new changes in the first place.

A similar issue arises in respect of certain third-party cookies. For example, if an end user consents to certain businesses using their analytics cookies on third-party websites, or similarly to use cookies for upvoting or liking content on other websites — will such consent apply across all third-party websites in which those cookies are used, or will the relevant websites need to obtain consent again if such cookies are used on their sites? If the former, it is unclear how both web browsers and websites would be able to determine whether such consent has been given, again potentially resulting in the need to obtain consent in any case.

In addition, it is currently difficult to predict how the concept of “necessity” will be applied under the current draft of the regulation, as this could severely impact many information society service business models. For example, if a free news website, as with most such sites, is funded by advertising revenues and uses cookies to display videos, which may or may not include advertisements, it is arguable whether such cookies are necessary for the provision of the service. If they are not, this would leave consent as the only alternative to use such cookies in accordance with the regulation. Given that the conditions for consent under the regulation are proposed to be the same as under the GDPR, we know that consent will be presumed to not be freely given if the provision of the service is dependent on the consent, despite such use of cookies not being necessary for the provision of the underlying service. While perhaps being economically necessary to use such cookies in this scenario, it is unlikely to be technically necessary; meaning any consent could be deemed invalid. The regulation therefore clearly threatens such business models if there is no valid way to legitimize the use of such cookies.

Furthermore, there is also the technical question as to how websites will recognize what cookie choices end users have made in their web browsers. This process may be facilitated by the key browser players agreeing on a common, universal standard, meaning websites would not have to code for each and every browser available. However, assuming the relevant players are amenable to this approach, this is a process that would likely take time, and may be difficult to reconcile with the commission’s aggressive timetable.
The above suggest that the “simplified” changes within the regulation may not actually provide for the “streamlined” mechanisms envisaged. We expect many businesses will lobby the commission on these points, requesting for rules that closer reflect the balance between commercial practicality and individuals’ rights. However, it remains to be seen whether this will result in any changes to the draft.

Conclusion

The regulation sets out to align the requirements of e-privacy and data protection in Europe for the benefits of the Digital Single Market initiative, with an aggressive timetable for implementation to coincide with that of the GDPR in May 2018. This combination of factors may not work in the draft’s favor. There is also a risk that in wanting to find an acceptable compromise EU Parliament may seek material changes in certain areas of the draft, which could delay the adoption of the regulation. However, there is clearly a desire to try and make this work and so much will depend on the exactly what pushback the EU parliament seeks.

As with the GDPR, the intention of harmonization is somewhat undermined by the number of derogations contained within the legislation giving each member state a general power to restrict obligations and rights where necessary and proportionate to safeguard general public interests. Therefore, it will be interesting to see if the EU Parliament seeks to restrain the scope and/or derogations contained in the draft or accept them to facilitate swift passage of this piece of legislation, relying on the jurisprudence of the CJEU to find a balance not set out in the regulation.

In parallel with preparations for the GDPR, and for those affected, the Network Information Security Directive, it would be wise to bear in mind the requirements of the regulation when reviewing policies, procedures and services in the next 12 months. If the regulation is adopted as intended, those taking this approach will mitigate the risks of the greatly increased administrative fining regime set out under both the GDPR and the regulation.
May 9, 2017

**The Information Commissioner’s Guidance on Consent under the GDPR**

The General Data Protection Regulation (the “GDPR”) came into force in May 2016 and makes numerous changes to European data protection laws. Among other things, the GDPR updates the rules on the use of consent by data controllers to justify their processing of personal data in various circumstances. The UK Information Commissioner’s (the “ICO”) consultation on its draft GDPR Consent Guidance (the “Guidance”) ended on 31 March 2017. The ICO reported on 13 April that over 300 responses have been received and these are now being analysed.

The draft Guidance is generally helpful and provides clear practical advice regarding many aspects of consent. However, there are some elements of the draft Guidance which are likely to prove contentious. It is clear that valid consent will become significantly harder to obtain and that it will often be more appropriate for data controllers to rely on an alternative legal basis other than consent to justify their personal data processing.

**What Has Changed?**

The Guidance confirms that the basic concept of consent and its main role as one potential lawful basis (or condition) for processing personal data has not changed; however, the GDPR builds on the existing definitions and standards of consent in various ways, setting a high standard for consent. Current methods of obtaining consent will need to be reviewed and refreshed. Clearer and more granular opt-in consent methods, good consent records and easy ways to withdraw consent will all be required.

The definition of consent set out in the GDPR includes additional requirements regarding how consent should be given. Consent is defined to mean “any freely given specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data relating to him or her” (emphasis added). The new elements of the definition are considered in more detail below.

For those involved in scientific research or processing children’s personal data online, there are new provisions on consent for scientific research purposes and children’s consent for online services. Consent and explicit consent, respectively, can also legitimise restricted processing and automated decisionmaking and profiling and international transfers of personal data if adequate safeguards are not in place. Consent can also give individuals stronger rights in some cases (e.g., the rights to data portability and erasure).

The ICO makes it clear that, if consents have been obtained previously, data controllers will not be required to refresh such consents if they meet the GDPR’s standards and have been properly documented, although they will need to implement mechanisms allowing individuals to withdraw their consent easily. In the light of the Guidance, it seems unlikely that many (if any) existing consent mechanisms will meet GDPR standards and, if they do not, fresh GDPR compliant consent will need to be sought. This may well involve significant work for data controllers who have historically relied on consent to justify their personal data processing.

**When is Consent Appropriate?**

A significant issue that the Guidance addresses is the fact that, under the GDPR, consent may well not always be required to provide a legal basis for processing personal data and may not always be the most appropriate basis or the easiest to achieve (there are six lawful bases for processing personal data, including consent). Essentially, data
controllers are likely to need to obtain consent when no other lawful basis is available, but it is less likely to be appropriate in other circumstances.

Consent will only be the most appropriate legal basis for processing when people are offered real and ongoing choice and control over how their personal data will be used. If a genuine choice cannot be offered, the ICO is clear that asking for consent could be considered misleading and unfair.

**Valid Consent**

The draft Guidance focuses on the various elements required to obtain valid consent. First, to ensure that consents are freely given, individuals must be able to refuse consent without penalty and withdraw consent easily at any time. Consents must be unbundled from other terms and conditions (with granular options provided for different types of processing) and not made a condition of receiving a service unless the relevant personal data processing is necessary for that service. For example, requiring individuals to agree to the use of their personal data for direct marketing purposes in order to receive a “free” online service, where the processing of personal data is not required for the individual to receive the service, is unlikely to be regarded as valid consent.

Employers and public authorities in particular should note that the Guidance also stresses that it will be difficult to obtain freely given consent in any relationship where there is an imbalance of power and they are likely to need to identify an alternative legal basis for personal data processing in many cases.

Of particular interest to data controllers involved in areas such as direct marketing is the fact that the ICO stresses that consents must specifically identify the data controller and any third party who will be relying on the consent and state the purposes of the processing. Consent for categories of third-party organisations will not be sufficiently specific. The requirement to specifically name each third party to whom personal data will be made available may well restrict certain data controllers’ ability to send direct marketing communications to potential customers.

Granular options to consent separately to separate purposes must also be provided covering each type of processing activity, where possible (unless such activities are clearly interdependent). Details of how to withdraw consent at any time must also be provided. Wording must be prominent, concise, separate from other terms and conditions and in plain language. For data controllers who wish to process personal data in various different ways for various different purposes, there may be a risk that complying with these requirements will confuse data subjects instead of clarifying the use of their data for them.

Electronic consent requests must not be unnecessarily disruptive to users, and the ICO recommends the use of user-friendly layered information and “just-in-time” notices. Data controllers are likely to have to make changes to their existing electronic consent procedures in many cases to ensure that these requirements are adhered to.

The GDPR requires it to be obvious that individuals have consented and what they have agreed to and a clear signal that they give consent is required. Clear affirmative action requires individuals to take deliberate action to opt in. The draft Guidance suggests that various forms of action will comprise a valid opt-in, for example, ticking an opt-in box (on paper or electronically), clicking a link online, signing a consent statement, making an equally prominent binary choice, or switching technical settings away from the default, among others. Relying on acceptance of general terms and conditions, failure to opt out, default settings, silence, pre-ticked boxes or inactivity will not constitute valid consent.

**Implied Consent**

The draft Guidance adopts a pragmatic approach to implied consent, confirming that it can still constitute an affirmative act in some circumstances, especially more informal offline situations, although it must also be possible to verify consent. The ICO has confirmed, however, that implied consent cannot be explicit consent.

**Duration of Consent**

Data controllers should note that consent is not static and that the validity of consent is contextual. Consents should be reviewed regularly as they will probably degrade over time, although this depends on the context, the scope of the
original consent and the data subject’s expectations. If processing operations change, consents may no longer be sufficiently specific or informed and data controllers will need to seek refreshed consents unless another lawful basis for processing exists, (as a default position, the ICO recommends considering refreshing consent every two years, but this may not always be appropriate).

The draft Guidance requires that withdrawal of consent should be an easily accessible one-step process and, if possible, data subjects should be able to withdraw their consent in the same way that they gave it (e.g., if consent is given using an online form, it should also be possible to withdraw consent using an online form). Data controllers should consider publicising both online preference management tools (such as privacy dashboards) so that individuals can access and update their consent settings easily and other easy ways of withdrawing consent (e.g., customer service phone numbers) and should also offer opt-out by reply to every contact (e.g. opt-out phone numbers, addresses or unsubscribe links in e-mails).

Children

For service providers targeting online services at children, the draft Guidance emphasises the new GDPR provisions which increase protection for children’s personal data and are additional to those already considered above. Subject to certain exceptions, if “information society services” (essentially, services requested and delivered over the internet) are offered to children and data controllers want to rely on consent as a lawful basis for processing, then consent from the child’s parent or guardian is required for any child under 16 (although Member States may impose a lower age not below 13). Data controllers will need to introduce age verification measures and must make reasonable efforts to verify parental responsibility for those under the relevant age.

Data controllers who process children’s personal data other than in the context of information society services should decide whether the child has the capacity to understand and consent for themselves. Age verification measures and steps to verify parental consent for children who cannot consent may still be needed. It is worth considering whether legitimate interests rather than consent could form a legal basis for the processing of children’s personal data in some circumstances.

Records

Data controllers will need to be able to show that individuals have consented to personal data processing, and effective audit trails of how and when consent was given should be established to provide evidence if challenged. The draft Guidance includes some useful examples of what consent records should include. Details should be kept of (i) who consented; (ii) when (e.g., the ICO suggests retaining copies of a dated document or online records that include timestamps); (iii) what they were told at the time; (iv) how they consented (e.g., if consent was given online, records should include the data submitted and a timestamp to link it to the relevant version of the data capture form); and (v) whether consent has been withdrawn and, if so, when. The Guidance suggests that records should also be specific and granular to show exactly what the consent relates to.

Comment

The Guidance sets out some helpful practical suggestions regarding how data controllers should obtain and manage consents in the context of personal data processing; however, some aspects of the Guidance may be controversial. For example, as noted above, there is a concern that the requirement to specifically identify every third party who will be relying on the consent rather than being able to list categories of third-party organisations will raise challenges for many data controllers. Similarly, there is a concern that the required level of granularity regarding opt-in mechanisms may, in practice, serve to confuse individuals rather than giving them enhanced choice and control over how they consent to the use of their personal data. Based on the draft Guidance, it seems likely that consent will be used by data controllers significantly less often to justify their personal data processing than has been the case prior to implementation of the GDPR. It will be interesting to see whether and, if so, in what ways, the Guidance is updated following the ICO’s consultation (the ICO hopes to publish the final version of the Guidance in June 2017).
BREXIT
As autumn approaches and preparation for the next round of Brexit discussions begins, this note summarises the current position and analysis following the UK’s vote to leave the EU on the 23rd June (the “Referendum”). Whilst the debate on the implications of Brexit, including the proposed shape and form of the UK’s new relationship with the EU is constantly evolving, it is clear that firms operating within the UK and the EU need to continue to do business throughout. Consequently, this note highlights steps that firms may wish to take during this interim period between now and the UK’s actual exit from the EU.

**“KEEP CALM AND CARRY ON”**

From a legal perspective, nothing has changed following the Referendum. The UK remains a member of the EU and applicable EU law remains in force. Although the outcome of the Referendum is not legally binding on the UK government (it is merely advisory), it appears highly unlikely that the UK Parliament will ignore the decision of the electorate. Consequently, this note sets out some of the potential legal implications which may affect your business upon Brexit.

There were various immediate economic consequences following the Referendum, including an initial fall in sterling and a decline in the stock market, but the UK economy has already shown signs of resilience following the immediate days after the Referendum. The UK government confirmed that it will relinquish its six month rotational presidency role of the European Council in 2017 with the President of the European Council (Donald Tusk) confirming that Estonia will take over this role.

In addition, Lord Hill resigned as the UK’s EU commissioner in the wake of the Referendum, and his role overseeing financial services regulation has been reassigned to Valdis Dombrovskis from Latvia. Consequently, although the UK remains a member of the EU until Brexit and maintains its position as having one of the largest GDPs in the EU, it is inevitable that the UK’s influence in current EU negotiations may diminish in the interim period prior to Brexit. Conversely, given that substantial pieces of financial services legislation (often based on UK principles of operation or UK legislation) have already been drafted and approved by the EU, the effective influence of the UK should continue within the EU financial services.

Despite the above, currently, it is “business as usual” in relation to day to day operations within the UK and the EU. However, businesses should monitor and track developments as the discussions and negotiations between the UK and the EU unfold and ensure amendments are implemented in future business plans. Firms may consider how to streamline...
their operations on a cross-border basis but also identify and take advantage of opportunities from the potential effects of the current market dislocation within the UK and EU.

**EXIT PROCEDURE AND NEGOTIATION PROCESS**

**Formal Exit Procedure**

Article 50 of the Treaty on European Union (“TEU”) sets out the procedure for a member state to withdraw from the EU. Article 50 states that a decision to leave should be made in accordance with a member state’s constitutional requirements. Once the UK notifies the European Council of its intention to withdraw under Article 50, the UK will remain a member of the EU until the earlier of: (a) the date on which an agreement to withdraw from the EU is finalised; or (b) the expiry of a two year period from the date of notification (unless there is unanimous approval for an extension from the other 27 EU member states). Under Article 50 the exiting member state cannot participate in discussions of the European Council regarding its exit.

The general view amongst commentators is that the withdrawal notice is irrevocable, as Article 50 does not provide for a revocation of the withdrawal notice, and therefore the trigger of Article 50 should not be used to renegotiate a member state’s position within the EU. (However, we do note that recent expert analysis, commissioned by the House of Lords, indicated that the decision to leave the EU can be reversed after an Article 50 notice had been delivered provided that this was prior to the withdrawal date.) Once the withdrawal agreement has taken effect, the decision to leave the EU is final. If the UK wishes to rejoin, it will need unanimous approval of all EU member states. Alternative options to implement the exit of the UK from the EU, such as treaty amendment under Article 48 TEU or repealing the European Communities Act 1972, have been put forward. These options are undeveloped and potentially more complicated. Furthermore, the European Council has made it clear that withdrawal should occur in accordance with the procedure set out in Article 50 and it seems unlikely that the UK will take an alternative route.

The withdrawal agreement requires approval by a qualified majority of the EU Council (being 72% of the member states representing at least 65% of the total EU population (excluding the UK)), which means that a single member state cannot block the vote. At this stage the shape and form of the withdrawal agreement (or agreements) is unclear, but will include technical details regarding allocation of surplus budgets, and other transitional issues. Decisions regarding the fundamental nature in which the UK and the EU work together going forward will be made, including agreeing on the future of the four EU freedoms and whether these will be upheld in any way. Questions will need to be answered as to whether there will be an agreement to maintain key principles such as the freedom of movement of people or the freedoms to provide goods or services across the EU if the UK were to leave the EU.

**Trade Relationships**

The UK currently trades with approximately 50 non-EU countries on the basis of preferential trade deals negotiated by the EU. As the UK will likely no longer benefit from these trade agreements following Brexit, it has started informal discussions for its own deals. Other trade relationships with around 100 countries are governed by World Trade Organisation (“WTO”) rules, which is the default position in absence of any other agreement. It would benefit the UK to negotiate more bespoke deals with these other countries. Technically under current EU rules, member states cannot enter into separate trade deals with either individual member states or third countries, therefore formal trade agreements can only be signed once the UK has left the EU. The government has three key members of the cabinet dealing with trade negotiations: the Brexit secretary (David Davis); the foreign secretary (Boris Johnson); and the international trade minister (Dr Liam Fox). The European Commission (“EC”) has appointed Michel Barnier, who was involved in Europe’s post-financial crisis, as its chief negotiator over the Brexit terms.

---

3 Sir David Edward KCMG, QC, PC, FRSE, a former Judge of the Court of Justice of the European Union and Professor of Law, University of Edinburgh; and Professor Derrick Wyatt QC, Professor of Law, Oxford University, and also of Brick Court Chambers.
Whilst the UK government has given every indication that it will implement Brexit there are a few issues under debate, which require resolution, in relation to the formal notification of Article 50 (including if and when the trigger will be invoked by the UK government).

**Constitutional Issues**

The UK government has not yet taken any steps to formalise the exit of the UK from the EU. While Theresa May, the new UK prime minister, has said “Brexit means Brexit”, there has been much debate as to whether formal withdrawal from the EU under Article 50 requires parliamentary approval to be constitutionally valid. Government lawyers have stated that withdrawal under Article 50 does not require an approval by the UK Parliament, but there are several pending legal challenges as to whether the Article 50 notice can be served by the government (acting through the prime minister) based solely on the exercise of royal prerogative. Some academics have argued that since the Parliament introduced EU law into UK domestic law, only the Parliament can trigger the steps to remove it. Others argue that the withdrawal decision falls under the government’s inherent prerogative powers to conduct foreign affairs. The use of prerogative powers to invoke Article 50 could be challenged as ultra vires if the authorisation of Parliament is not sought. We note that the UK Prime Minister and her cabinet have indicated they do not intend to seek prior parliamentary approval or require a general election prior to triggering Article 50.

**Timing**

The UK government has indicated that it will only invoke Article 50 after further domestic consideration and analysis has been undertaken in relation to the exit process, and that it is unlikely to occur before the end of 2016. Commentators have discussed that the timing of the submission of the formal notice under Article 50 may also be influenced by general elections in Germany and France in 2017. Despite the lack of a formal ‘trigger’, the UK government has begun its efforts to engage with leaders of EU members states informally, though it should be noted that key EU leaders and Members of European Parliament (“MEPs”) have stated that minimal negotiations (or decision making) may occur prior to the UK serving the Article 50 notice and commencing formal discussions. Aside from discussions at the government level, there are further informal discussions between UK institutions and their counterparts in other EU jurisdictions (including at a regulator to regulator level), primarily with the aim of ensuring a smooth continuance of business now and preparing for an effective transition of relevant legal entity permissions if and when this may become necessary.

---

### POTENTIAL MODELS FOR THE FUTURE RELATIONSHIP OF THE UK WITH THE EU

The European single market guarantees the “four freedoms” in the EU-free movement of goods, persons, capital and services. The UK may seek to maintain certain aspects of these arrangements with the EU, while negotiating to remove less advantageous aspects. The UK’s continued access to the EU single market following Brexit appears, to a certain extent, to depend on the continuation of all four freedoms.

There are a number of more “established” options available to the UK on exit from the EU including:

- **Membership of the European Economic Area (“EEA”)** and **European Free Trade Association** (“EFTA”) (such as Norway). This allows access to the EU’s internal market without a vote on policy or law-making and requires a financial contribution to the EU budget (the “Norwegian Model”). To become a member of the EEA, the UK would need to re-join the EFTA to enable it to benefit from the economic co-operation, free movement of goods between the EFTA states (Iceland, Liechtenstein, Norway and Switzerland) and also possibly access the EFTA’s existing free trade agreements with over 35 countries;

---

4 EEA membership is available to member states of the EU and EFTA.
5 The UK historically was a member before leaving to join what is now the EU.
- **Customs union** (such as Turkey). This allows limited access to the single market for goods, but not services;

- **Bilateral arrangements with the EU** (such as Switzerland). This provides access in part to the EU single market and requires a financial contribution to the EU budget. Negotiations with Switzerland were lengthy and resulted in over 200 trade agreements;

- **Free trade agreement** (such as Canada). This would be a more bespoke option with a trade agreement between the UK and the EU bloc, but could take time;

- **Continuing membership of World Trade Organisation** (“WTO”). This would rely on general international trading rules, which would be the default model if no other agreement was reached between the EU and the UK; or

- **Renegotiation of the EEA Agreement**. An alternative approach has been suggested where the UK could re-join the EFTA and then attempt to renegotiate the EEA Agreement with the EU as a bloc with the other EFTA member states.

However, there is also the possibility that the UK will aim to craft a “UK specific” agreement which may be an amalgamation of elements of the options stated above. Again, it is hard to predict which approach the government is likely to take at this stage.

**WHAT DOES BREXIT MEAN FOR THE CITY OF LONDON?**

Much has been written about the effects of Brexit and how it could impact London’s position as the EU’s principal financial centre if the UK loses its access to the EU single market and associated “passporting” rights. The use of the EU passport allows a firm to establish in one EU jurisdiction and obtain a passport to provide services in another EU jurisdiction. This can be achieved either on a cross-border basis or through establishing a branch. The use of passporting is discussed in more detail below in the “Regulatory” section, as well as in our separate client briefing on passporting, available here.

However, it should be noted that financial services are a major part of the UK economy (around 10% of UK’s gross domestic product) and London’s established capital markets account for about three quarters of European capital market business. These factors, along with the sophisticated legal regime, language advantages and the geographical appeal of London have made the City attractive as headquarters for European financial activity and business. The City is home to key personnel, with a wealth of specialist expertise, who may be reluctant to leave London. Consequently, despite that announcement of certain banks that the possible loss or partial loss of the EU passport may result in a downsizing of their London operations and trigger a move of certain functions to other EU countries or even the United States, we are of the view that London will continue to have much to offer within the global financial services industry. We also note that differing financial services entities and sectors will approach Brexit differently, with some industries such as the asset management industry recognising that in many instances they already have operations set up in both the UK and Continental Europe, diluting the potential effect of Brexit on existing operations.

London’s appeal to international litigants should remain unaltered following Brexit. The popularity of the English courts as a forum of choice in international transactions should continue due to their efficiency, accessibility and record of impartiality. English contract law is largely unaffected by Brexit and is likely to retain its prevalence as the governing law for international contracts, as its relative predictability (due to precedent case law), commerciality and familiarity will remain attractive.

**KEY CONSIDERATIONS**

Whilst it is still too early to provide a definitive legal analysis of the effect of Brexit, firms should begin their analysis on the potential impact of Brexit on their business. The remainder of this note provides more detail in relation to some of the key areas that may affect businesses and sets out some issues that will need to be monitored as the Brexit discussion progresses.
**Impact On Contracts**

Whilst we believe that it is unlikely that Brexit will have a significant impact on the interpretation and enforceability of existing or new contracts governed under English law, it will still be necessary to conduct further analysis in the coming months on the potential consequences of Brexit on contracts governed by English law.

**Governing Law, Jurisdiction And Enforceability**

The choice of governing law for new contracts may be a consideration for lawyers and businesses following the Referendum but the possible changes have, in the main, in our view, been overstated. The concern is that leaving the EU will mean that English courts are no longer bound by the Rome I Regulations6 and the Rome II Regulations7 which currently require member states’ courts to respect an agreed choice governing of law clause (which will mean that the other member states will continue to give effect to English law contracts). However, even if the UK reverts to English common law without entering into a new arrangement with the EU, the common law had a solid history of upholding parties’ choice of law. Where the parties have not specified a governing law, the principles that would be applied under English common law are broadly similar to those that would be applied under the Rome I & II Regulations. Given the courts’ willingness to uphold governing law clauses, the most effective way to remedy any uncertainty surrounding governing law is to include an explicit governing law clause in all contracts.

In contrast to governing law, Brexit does raise questions about the appropriate jurisdiction arrangements post-Brexit when parties have not specified jurisdiction in commercial agreements. At present, the Brussels I Regulation (recast)8 details how jurisdiction should be determined including factors such as the location of defendants and the place where the “harm” occurred. The Brussels I Regulation also introduced the current enforcement framework for the EU, allowing the enforcement of member state judgments in any other member state without any need for further hearings. Brexit will mean that the UK is no longer part of the Brussels I Regulation. The UK may seek to join the Lugano Convention or the Hague Convention on Choice of Court Agreements (which goes even further geographically than the Brussels I Regulation and includes Singapore and Mexico) to try and preserve the status quo as much as possible, but these agreements do not provide the same level of protection as the Brussels I Regulation. Crucially, the UK will need to find an agreement that means that English judgments can be enforced, without delay or additional cost (for example having to sue on a judgment), in the other EU member states in order to stem any potential flow of litigation on to the continent.

**Contractual Clauses**

A further discrete point is whether or not parties may consider challenging the validity of contracts on the basis that Brexit represents a force majeure. For example if tariffs are imposed between the EU and UK that significantly change the nature of an agreement, it will be a matter for the court to decide if Brexit can be considered an “exceptional event”. Timing of agreements will be crucial in this regard because in order to successfully argue that an event is a force majeure it must be unforeseeable at the date of the contract. In practice, it will be difficult for a party to argue that Brexit was unforeseeable following the Conservative Party’s election win in 2015.

Contracts which reference the EU as a territorial jurisdiction may also be the subject of review following Brexit. For example, this will be most relevant in distribution agreements where parties may wish to consider amending terms, where possible, to specifically include or exclude the UK.

**Next Steps?**

Whilst there is probably no need for a comprehensive document review at present, it would be prudent to consider documentation which may warrant a deeper analysis to identify any potential key issues regarding governing law or the potential trigger of force majeure or material adverse change, or review key contracts which may include references or reliance on the existence of EU/EEA laws or EU/EEA/EFTA membership. In addition, it may be useful to insert “Brexit proof” clauses either

---

6 EC/593/2008
7 EC/864/2007
8 EU/1215/2012
by amending existing key contracts or when entering into new contractual documentation. In relation to financial services, there is already a concerted effort to pool together thought on drafting “Brexit proof” clauses and/or concepts of grandfathering provisions, particularly in relation to references to the applicability of EU Directives or Regulations.

**Impact On The Use Of The Financial Services Passport**

While it is uncertain which model the UK will adopt following Brexit, for now (and unless a “UK specific” alternative is found) only UK membership of the EEA would guarantee the continued use of EU/EEA passporting rights for regulated financial services firms (the “EU/EEA Passport”). Under certain Directives, the UK could obtain passporting rights (in respect of some services and for some types of clients) as a “third country”, conditional on the UK’s financial services regime being determined to be equivalent by the European Securities and Markets Authority (“ESMA”) (the “3rd Country Passport”). Please see our previous client alert and blog on passporting for a more detail.

The availability of a passport varies under each EU Directive, with some Directives such as the Markets in Financial Services Directive II (“MiFID II”) and the Alternative Investment Fund Managers Directive (the “AIFMD”) providing for the availability of both an EU/EEA Passport and a 3rd Country Passport, whilst the Capital Requirements Directive IV (“CRD IV”) does not contemplate for a 3rd Country Passport and the Undertakings in Collective Investment Schemes Directive (“UCITS”) does not allow for third country access either. Consequently, firms will need to conduct an analysis on which of its entities is affected under a potential Brexit and what potential options they have available to them if the UK is no longer part of the EU/EEA. From a timing perspective, whilst it is too early to set out in stone what the future relationship the UK will have with the EU, in the next few months and likely before a Brexit occurs, firms will need to start forming views as to what steps (if any) they need to take to ensure they can carry out their business plan effectively within the UK and the rest of the EU going forward.

This decision making may vary depending on the types of activity your entity conducts and what other entities you have in the EU outside of the UK. For example, whilst there may not be an immediate need for a firm which has established both a retail fund platform in the UK and the EU to change anything other than to monitor whether their EU entity will be allowed to delegate certain functions to the UK entity, this may not be the case for banks headquartered in the UK who rely on their EU/EEA passport to conduct banking services.

**Obtaining Passport On The Basis Of ‘Equivalence’**

If the UK leaves the EU (and is not a member of the EEA either), it would be treated as a “third country” for the purposes of EU financial services legislation. As indicated above, some EU Directives grant rights to third country firms to conduct business in the EU on the same basis as EU firms, namely MiFID II, the AIFMD and the Solvency Directive. The question of what meets the criteria for “equivalence” is likely to draw much attention over the coming months and years, particularly as (at present) there is no uniform approach to equivalence across all EU Directives. In addition, the concept of equivalence is fairly new under EU legislation; consequently, it is hard to draw firm conclusions on what tests the UK will need to complete to meet the equivalence test under each EU Directive that provides for a 3rd Country Passport. It is useful to look at the commentary provided by ESMA for the purposes of the use of the 3rd Country passport under the AIFMD detailed below as at least an initial indicator of what may be expected by the EU (please see our client alert on the AIFMD 3rd Country passport).

However, the story of equivalence may not be that simple when we look at the terms set out in ESMA’s advice on the AIFMD, which reviewed whether there was a level playing field for competition between the EU and a third country. For example, if the UK were to opt for a “twin track” approach, allowing for parallel tracks for firms to operate or products to be sold in the UK with one set being held out as “EU equivalent” and another set of domestic “regulatory–light” rules for UK firms, a question would open up as to whether this would meet ESMA’s criteria for a level playing field for competition purposes?

MiFID II envisages a regime to allow third country firms to provide cross-border services covered by MiFID (such as broker-dealer services) only to more sophisticated or institutional EU clients (namely, per se professional
clients and eligible counterparties). This regime will only be implemented at some point following the application date of MiFID II, January 2018. The principle condition is that the EC adopts an “equivalence” decision in relation to the relevant third country if the EC determines that the third country has prudential and business conduct rules which have equivalent effect to the CRD and MiFID (and the detailed implementing measures made thereunder). The EC must also determine that the third country has an effective equivalent system for the recognition of foreign investment firms. On the assumption that the UK will largely retain the same rules as under CRD and MiFID, the UK’s regime may be considered “equivalent” at some date in the future, but this is not certain – particularly if the UK sees a competitive advantage in diverging from some aspects of CRD and MiFID in the future. In addition, there is no particular timetable for the Commission to adopt an equivalence decision. In the meantime, local rules on access by third countries will apply which can be restrictive.

There is no third country passport under MiFID for services provided to retail clients (including individuals and local authorities (and potentially their pension schemes). MiFID allows member states to require any third country firm to establish a branch in the state the service is provided. In practice, third country firms that intend to actively solicit business from retail clients in more than one or two member states will need to establish a separate entity in one state, obtain authorisation for that entity and use the MiFID passport to provide services in all other states.

The grant of the passport under AIFMD to third country firms is at a more advanced stage. ESMA recently published its final advice to the EC, giving the green light to the grant of the passport to managers and funds established in (inter alia) the United States, Guernsey, Jersey, Switzerland and Japan. The conditions in the AIFMD for the grant of the passport are similar (but not identical) to the conditions in MiFID. ESMA’s work to date indicates that the key conditions are, firstly, that the third country’s regime is suitably robust in terms of supervision and investor protection, and, secondly, that there is a level playing field between EU and non-EU managers as regards market access, in particular whether the third country regime allows marketing by EU managers of their funds on reasonable terms. If the UK retains its AIFMD rules (potentially as an “opt-in” for UK managers), there appears to be no reason why the UK cannot obtain the third country passport – but this is in part a political decision, raising uncertainties as to the criteria which the EC might apply.

**Tax**

The EU oversees national tax rules to ensure that these are compatible with EU law and policy, but tax rate setting and tax collection generally remains a matter for individual member states. The direct impact of Brexit is likely to be felt only in those areas where the UK regime originates from EU law (such as VAT). Other aspects may change following Brexit, for instance following extrication from EU state aid restrictions and the single market. Much will depend on the precise UK-EU relationship post-withdrawal, and (as always in fiscal affairs) the prevailing economic climate and impact of Brexit on HM Treasury revenues. Implementation of the OECD’s Base Erosion and Profit Shifting project (“BEPS Project”) is entirely separate to the question of the UK’s EU membership and the changes in law arising from the BEPS Project are not expected to be affected by the UK’s withdrawal. However, on leaving the EU the UK would not, prima facie, be obliged to implement the recently approved EU Anti-Tax Avoidance Directive, or any other EU measures, aimed at harmonizing the implementation of the BEPS Project throughout the EU, other than by virtue of any terms relating to the UK-EU relationship post Brexit.

**Value Added Tax**

The VAT system within the EU (UK included) is broadly aligned under EU law. As a large and well established source of revenue for HM Treasury, there is a strong incentive for the UK to maintain alignment with the EU system immediately following withdrawal. However, the UK would also gain the ability to adjust rates and alter VAT exemptions/reliefs after Brexit.

Some implementation and compliance costs of transitioning to any new domestic VAT system should be anticipated. Some areas could be simplified, such as removing the current requirement to submit European Sales Lists of intra-EU B2B supplies. However, there may be a cash flow cost for importers in paying and recovering import VAT on goods received from other EU member states.
Withholding Tax/Double Taxation

The UK has an extensive network of double tax treaties ("DTTs"), which operate to reduce or eliminate a number of instances of double taxation and the imposition of withholding tax on certain payments made to and from the UK. The Referendum and Brexit are not expected to affect their operation. As it currently stands, these DTTs are overlaid by two key Directives that eliminate withholding taxes on certain dividends, interest and royalty payments made between associated companies within the EU. In addition, double taxation of dividend payments between parents and subsidiaries within the EU is prevented. Fully outside of the EU, payments made intra-group to and from the UK/EU will cease to benefit from these Directives.

In many cases, the relevant DTT should provide equivalent relief to the Directives, but there are cases where coverage from the relevant DTT is incomplete. This could affect (i) interest payments between certain jurisdictions such as the UK and Italy and Portugal (and vice versa), and (ii) relief from withholding tax on dividends paid to the UK out of certain jurisdictions such as Austria, Germany, Italy and Portugal. In addition (unless a domestic participation exemption applies), domestic tax charges for dividend income received by an EU parent entity from the UK may not be fully eliminated under the relevant DTT.

Recent UK draft legislation\(^9\) increases the scope for UK withholding tax on royalties, to include payments from non-UK companies “in connection with a trade carried on by that person through a permanent establishment in the UK”. The UK DTTs with, for example, Luxembourg, Italy and Portugal do not give zero rates on withholding on royalties, so both payer and recipient companies should consider whether a UK withholding tax liability would arise under these new rules.

In addition, certain US DTTs with EU member states, such as the Luxembourg–US DTT provide an exclusion from the limitation of benefits clause where, inter alia, 95% of a company’s shares are owned by seven or fewer EU (or in certain cases, EEA) companies. Following Brexit, unless something changes in these DTTs, subsidiaries of UK parent entities will lose this protection.

Additional areas to consider

On occasion, other aspects of the UK’s direct tax regime have been held to be incompatible with EU law. A stamp duty reserve tax of 1.5% on UK company shares issued into depository receipt and clearance systems (e.g. Euroclear, Clearstream etc) could be applied, along with the introduction of targeted tax incentive regimes that might previously have been considered as unlawful state aid. Conversely, the UK is likely to lose ‘protection’ from being discriminated against by other member states. If the UK is no longer bound to respect the EU fundamental freedoms, we may also see a broadening of the current UK Controlled Foreign Companies rules. With the UK outside of the EU, developments towards the EU Financial Transactions Tax and Common Consolidated Corporation Tax Base could be accelerated.

Transaction documentation will need to be carefully considered to ensure the risks from changes in law arising from the UK’s departure are considered and adequately addressed. The impact of Brexit on the eventual enforcement of judicial tax decisions that involve questions of EU law is also in question, although current and future litigation will of course be decided on the law in force at the relevant time.

Cross-Border Insolvency

The EU Insolvency Regulation\(^10\) ("EIR") is currently directly applicable in the UK. Its successor, the recast EU Insolvency Regulation\(^11\) ("recast EIR") will apply to proceedings commenced on or after 26 June 2017, until the occurrence of Brexit. Both regulations focus on the allocation of jurisdiction between the courts of member states, with a view to minimising or entirely avoiding competing proceedings. It remains to be seen whether the continued application of the EIR or the recast EIR can or will be negotiated, once the UK leaves the EU.

Existing alternative provisions are of limited assistance. The Insolvency Act requires the UK courts having jurisdiction in relation to an insolvency court to assist courts having the corresponding jurisdiction in “any relevant country or territory”, but a) that provision only assists in relation to inbound requests to UK and b) no member state is currently designated a “relevant country or

---

\(^9\) Once enacted, the rules will be backdated to apply from 28 June 2016.

\(^10\) EC/1346/2000
“territory”. The UK’s Cross-Border Insolvency Regulations\textsuperscript{12}, implementing the UNCITRAL Model Law, provide for co-operation and recognition between courts and competent authorities involved in cases of cross-border insolvency, but again, this will only assist with inbound requests, as only Greece, Poland, Romania and Slovenia of the other member states have signed up to UNCITRAL.

### Schemes Of Arrangement

Over the past 10 years, the restructuring of companies incorporated in member states other than the UK via schemes of arrangement sanctioned by the UK courts has become increasingly popular. While the EIR and the recast EIR have no application to schemes, it is arguable that the EU Judgments Regulation\textsuperscript{13} does apply. This is relevant for two reasons. First, it has been argued that its conditions need to be satisfied to establish the jurisdiction of the UK court to sanction a scheme. That argument against scheme jurisdiction could no longer be run if the Judgments Regulation ceased to apply to the UK. Second, it has been argued that the UK court’s decision will be recognised in other member states because the Judgments Regulation applies. That is crucial where most of the company’s assets are in other member states, as the court wants to be satisfied that its sanction order will have substantive effect. While that argument in favour of jurisdiction could no longer be relied upon, evidence that the order would be recognised on local or private international law grounds has already been accepted by the UK courts in a number of cases covering the key EU jurisdictions other than the UK. Consequently, while it remains to be seen whether the continued application of the Judgments Regulation can or will be negotiated, schemes of arrangement should largely be unaffected.

### Arbitration

In the short-term there may be an increase in the popularity of Alternative Dispute Resolution. In the UK this may lead to more parties seeking to mediate their disputes, but in terms of international disputes, arbitration is likely to be a more suitable option given the inevitable uncertainty of the English legal system for the next few years. Arbitration may be particularly attractive to claimants whose counterparties have assets located in jurisdictions where an English judgment would not be enforceable, such as Russia. The reason for this is that the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards has a much broader reach and therefore offers enforcement protections even wider than the Brussels I Regulation. There is also the potential for English litigation to be slow and costly as the courts wade through the new framework and, as a result, arbitration is likely to be considered a solid option for disputes in the short to medium term.

### Private Equity Transactions

Following the Referendum very little has changed or is likely to change in terms of the legal framework for carrying out private equity transactions in the UK. Ultimately, this is a matter of domestic (and not EU) law. Implications following Brexit from a tax structuring and merger control perspective should also be considered in PE transactions (and these are discussed separately in this note). By way of contrast, the uncertainty surrounding the terms of the UK’s continuing relationship with the EU and the likely timeframe for concluding these negotiations has had a significant impact on market confidence.

From a legal perspective at this stage, it is not possible to provide much clarity as to the legal framework that will apply to UK businesses. That said, from a legal due diligence perspective, there are strategies that can be developed to help navigate this uncertainty in terms of assessing the impact that Brexit might have on possible UK-based investment targets for a PE purchaser (or, indeed, for a vendor diligence piece in respect of existing portfolio companies). Even at this stage, it is possible to identify those sectors and businesses that are more vulnerable in certain Brexit scenarios. Obvious examples of these would include any business with significant cross-border sales of goods or services, which will need to consider the potential impact of customs tariffs, if the UK loses access to the single market. Equally, any

\begin{footnotes}
\item EC/1346/2000
\item SI 2006/1030
\item EC/1215/2012
\end{footnotes}
business whose workforce relies heavily on non-UK EU citizens may be impacted if any UK exit treaty involves restrictions on such EU citizens coming to (or continuing to) work in the UK.

Monitoring the UK’s negotiations with the EU and how the UK’s exit deal is likely to be structured will be crucial. As this process evolves, any potential investment in a target with UK operations will need to involve a careful analysis as part of the legal due diligence process to assess how its business may be affected by changes in law or regulation following Brexit. Furthermore, as we get closer to the date of the UK’s exit, transaction documents may include specific provisions relating to Brexit and its implications.

Real Estate
property laws in the UK are fundamentally domestic systems and consequently Brexit should have a very limited legal effect on UK real estate transactions. Where EU laws impact on UK real estate, such as some environmental and planning legislation which has been implemented into domestic legislation, the expectation is that this legislation will remain in effect post-Brexit.

For the broader UK real estate sector, it is too soon to draw any meaningful conclusion on the long term impacts (if any) of Brexit. In the short term however, there is some market reaction as a result of concerns, for example, over occupier demand, the future viability of some development schemes and a fall in valuations.

In addition, a number of UK open ended real estate funds have restricted redemptions (“gates”) to protect the funds’ cash buffers and consequently liquidity has been exhausted. Investors have sought to redeem their investments following fund managers revaluing their portfolios after the Referendum. To date, the funds concerned hold a combined estimated total of £15 billion of UK property and industry analysts estimate that £3 billion to £5 billion of those assets could be put up for sale and these assets are likely to be subject to a discount.

There are undoubtedly opportunities for overseas investors to take advantage of the pressure on sterling, low interest rates and Brexit discounts on assets. A large amount of capital has been raised in recent years to invest in UK and European real estate and therefore a number of private equity real estate investors are primed to invest in discounted UK real estate in the next six to eighteen months, including from those property funds which have suspended trading.

Loan And High Yield Bond Market
The Referendum result does not trigger any immediate legal issues for loan and bond deals whilst the UK remains part of the EU. Due to the expectation that Brexit is unlikely to occur before the end of 2016 (and the assumption that there will be a two year window once Article 50 is served), the Referendum result appears to have had minimal impact on the loan and bond market at this point.

Commitment Paper Terms

- Flex
  Prior to the Referendum there was discussion of flex terms linked specifically to the Referendum, to enable lenders to re-price or restructure the deal to optimise syndication. These were largely resisted with strong borrowers suggesting the risk should have already been priced into the deal. In the aftermath of the Referendum flex terms appear to be based on the standard risk analysis. In the future this risk analysis may include the invocation of Article 50 and the actual event of Brexit two years later, whilst taking into account the term and timing of the commitment period.

- Leverage
  Currently issues such as excess demand from the buy side, quantitative easing and other actions by central banks, and US leveraged lending guidelines are more likely to influence leverage levels rather than the prospect of Brexit.

- Pricing
  Recently increased search in the market for yield has influenced pricing more predominantly than concerns related to the Referendum. In the weeks following the Brexit vote, a number of deals priced in the market at levels lower than pricing indications provided prior to the Referendum and there have also been some reversed flexed deals. However, we will need to wait post-summer to see a more accurate state of the market and pricing levels.
**Foreign Exchange Issues**

In respect of borrowers with sterling revenue but euro or dollar denominated debt and/or multi-currency operating costs which are unhedged (or insufficiently hedged), fluctuations in the value of sterling (including the significant drop following the Referendum) could have an impact on the cash flow of a company as well as the financial covenants. Financial statements for the period ending 30 June 2016 may adversely affect financial covenant ratios if a spot rate is used rather than an average exchange rate for these UK businesses. The possibility of further currency movements and exchange rate risks may result in borrowers revisiting their financial covenants and also assessing whether further hedging would be prudent. The potential increased cost of borrowing sterling and uncertainty in the European loan market may make “Yankee loans” more appealing to European borrowers who can accommodate the exchange rate costs of borrowing in dollars.

**Tax Implications**

Borrowers should consider the tax implications resulting from their EU group structure. Finance transactions are typically structured to eliminate withholding tax by ensuring lenders qualify for exemptions and the borrowers are therefore not obliged to gross-up their interest payments. These exemptions are generally governed by domestic law, but in certain circumstances the domestic exemption links to EU law and therefore on Brexit may no longer provide relief on withholding tax. In many cases the relevant DTT will provide an equivalent exemption, but some DTTs do not completely eliminate withholding tax. The impact of Brexit on tax issues are discussed further in this note above.

**Drafting Considerations**

Bond issuers could consider the inclusion of a risk factor in their bond documents warning that market volatility and uncertainty resulting from the Referendum may have an impact upon earnings and ability to access the credit markets. Exposure will be greatest with companies where there is a significant UK business or other UK exposure.

Various Loan Market Association (“LMA”) provisions will require additional scrutiny, possibly requiring amendments to existing documentation as well as consideration for new financing arrangements. Typically a loan document includes various covenants linked to a business material adverse change clause, which generally should not result in the Referendum or Brexit triggering a specific event of default which would ultimately allow the lenders to accelerate the debt. Lenders have historically been reluctant to call a business MAC, as it is highly subjective and a direct causal link is required between the event and adverse effect on the business of the borrower group as a whole. Going forward, caution should be exercised when drafting a MAC clause which specifically contemplates Brexit as case law precludes lenders from invoking a MAC if the parties could have anticipated the adverse events at the time of drafting the provisions.

The loss of the EU passport may create issues for UK lenders providing funding to EU entities following Brexit, unless separate licences have been negotiated where necessary. A practical solution may be for a UK financial institution to lend the funds through one of its facility offices in the EU. Illegality provisions in existing loan documentation may be triggered on Brexit requiring prepayment and cancellation in respect of a lender’s commitment, so drafting to enable replacement at par, or the flexibility for the lender to transfer the loan to an EU authorised affiliate should be considered (if not already included).

Industry bodies such as the LMA, the Association for Financial Markets in Europe and ESMA are monitoring developments and will attempt to address issues that arise in relation to the finance market. The LMA recommended forms of financing documents contain specific references to EU regulations and directives, although the interpretation provisions qualify that these references are to those laws as amended or re-enacted, which should minimise the impact of potential legislative change upon Brexit. Certain clauses (e.g. the representation relating to COMI and the increased costs clause that refers to CRD IV) may require further amendment when the UK leaves the EU. The LMA will also incorporate any new or replacement laws into their standard forms in due course. In relation to the Bank Recovery and Resolution Directive (“BRRD”), on Brexit EEA lenders will need to include a contractual recognition of bail-in provision in relevant English-law-governed contracts.
Securitisations And CLOs

EUR CLOs, the vast majority of which are managed by UK firms, provide around 30% of the funding to non-investment grade borrowers in the EU. The majority of EUR CLOs are managed by UK MiFID firms which qualify as “sponsors” under the Capital Requirements Regulations (“CRR”) and in this capacity they are eligible to act as risk retainers under the CRR. If the UK does not join the EEA and where ESMA has not otherwise recognised the UK regulatory regime as “equivalent” for the purposes of MiFID II, UK managers would no longer qualify as ‘sponsors’ under the CRR and so would cease to be eligible in this capacity to act as risk retainers in respect of the EUR CLOs which they manage.

Manager Originator Structures

For new transactions, it is possible for a UK manager to “Brexit proof” the structure by changing from a “sponsor” risk retention structure to a “manager originator” structure which does not require the manager originator to have an EU or EEA regulatory status. This structure has already been used by some US managers since 2015 to enable them to market USD CLOs to EU regulated investors. The manager originator structure, as well as requiring the manager originator to manage the CLO, also requires that the manager originator contributes some of the loans or bonds which are acquired by the CLO issuer. The CRR and the delegated regulations thereunder do not prescribe a minimum percentage of loans or bonds which must be contributed by a manager originator (whereas the alternative originator structure, the “non-manager originator” structure, requires non-manager originators to contribute over 50% of the loan or bonds); prior to the Brexit vote, a number of USD CLOs were sold to EU regulated investors with the manager originator contributing 5% of the CLO’s assets and since the Brexit vote, the expectation is that more manager originators will come to market having contributed around 5% to 10% of the loans or bonds. There has been some discussion of manager originators contributing less than 5% of the loans or bonds which is possible under the CRR delegated regulations though some investors may prefer a higher level of contribution. The manager originator structure does not require the manager originator to take market risk in the loans or bonds which they contribute: the requirement is that the manager originator be exposed to the credit risk of the loans or bonds before they settle into the CLO issuer. There is no prescribed minimum holding period, but 15 business days has been seen as the period of credit risk in a number of transactions.

Regulatory Changes

In addition to Brexit, the securitisation and CLO markets are also due to be regulated under a new Securitisation Regulation promulgated by the EC as part of the Capital Markets Union initiative (sponsored by UK’s former EU commissioner). Under the EC’s draft Securitisation Regulation (as approved by the EU Council), the main change proposed to the risk retention regime is the additional requirement that originators established or operated for the “sole purpose of securitising exposures” would not be eligible to act as risk retainers: this requirement (if enacted) would not cause issues for manager originator structures which have the economic purpose of receiving management fees in addition to acting as risk retainer (this new test would however require non-manager originators to demonstrate their economic purpose beyond acting as risk retainer). Prior to the Referendum MEP Paul Tang unexpectedly proposed some significant amendments to the draft Securitisation Regulation including proposals (i) to increase the risk retention requirement from 5% to 20% and (ii) to limit eligible risk retainers to EU regulated entities. The EC has since attempted to reassure the market that they do not support increasing the risk retention requirement. The Tang proposal to limit eligible risk retainers to EU regulated entities would however cause issues for UK manager originator structures (in the absence of the UK remaining in the EEA or otherwise having its regulatory regime deemed equivalent once MiFID II is in force).

Existing sponsor transactions are expected to be grandfathered but if there is imperfect grandfathering which does not extend to secondary market purchases, this would be an issue for EU investors, who might ask UK sponsors to redeem legacy deals by refinancing via new manager originator structures.

---

14 A major debt fund has already priced a manager originator structure in the weeks following the Referendum.
UK securitisations involving a single originator acting as risk retainer (for example most RMBS, credit card, auto and corporate securitisations) will continue to be eligible as non-manger originator risk retainers in a full Brexit scenario but, as with CLO manager originator structures, they would also require restructuring (if marketing to EU regulated investors is required) if Tang’s proposal, to limit risk retainers to EU regulated entities, is implemented.

**Derivatives**

European Market Infrastructure Regulation (“EMIR”) stems from commitments made by the G20 nations in 2009, and it will therefore need to be replaced in the UK by a similar piece of national legislation on Brexit. Under EMIR, OTC derivatives can be cleared through an authorised EU clearing house (“CCP”) or a non-EU CCP that has been “recognised” by ESMA. An equivalence determination by the EC is a precondition to non-EU CCPs of a particular jurisdiction being granted recognition, therefore a key question will be whether UK CCPs will be granted recognition under EMIR following Brexit. Another question is the extent to which non-UK CCPs (e.g. US or EU CCPs) will be granted recognition under any UK version of EMIR. A reciprocal system for recognising overseas CCPs is required in order to gain the equivalence determination by the EC. Under EMIR, “substituted compliance” with the requirements of another jurisdiction is possible if an equivalence determination has been made by the EC in relation to that jurisdiction and at least one of the parties to the derivatives is established in that jurisdiction. At this point we do not know if an equivalence decision will be made in relation to any UK regulatory regime that replaces EMIR (no equivalence determinations of this type under EMIR have been made by the EC to date.) A similar question will arise under any UK version of EMIR: will it be open to the parties to comply with the EU or US requirements instead?

Other issues affecting derivatives that will need to be monitored include: (i) choice of law/courts; (ii) BRRD e.g. bail-in clauses; (iii) Financial Collateral Directive, and the associated UK regulations; and (iv) insolvency, especially the Credit Institutions Winding-up Directive.

**Competition**

The impact of Brexit on the merger control process for M&A transactions involving a UK component will very much depend on the post-exit model chosen. For merger control purposes, the key distinction will be whether the UK adopts:

- the Norwegian Model following the model adopted by Norway, Liechtenstein and Iceland, which is implemented through the EEA and EFTA agreements and allows the EC to retain exclusive competence over merger control transactions with EEA-wide impact; or

- any of the other models currently under discussion (the so-called Swiss, Canadian, Turkish and WTO models as detailed above), each of which would result in the UK coming out of the EU merger control regime.

If Brexit takes the form of the Norwegian Model, it will largely be business as usual: the EC would retain exclusive jurisdiction for mergers with an EU dimension, whilst the UK’s Competition and Markets Authority (“CMA”) would retain its current role for transactions that do not qualify for EC review.

If Brexit follows any of the other models, the EC would no longer have exclusive competence for merger control in relation to concentrations impacting UK trade. Depending on whether jurisdictional thresholds are met, this could result in the CMA and the EC having concurrent jurisdiction to review certain transactions. Overall, this would likely result in a greater filing burden and cost for private equity buyers than under the current one-stop shop regime, although the impact on individual transactions would be fact-specific: in practice, for as long as the UK’s merger control regime remains voluntary and non-suspensory, a private equity acquisition which does not give rise to UK competition concerns should continue to proceed without a UK filing. However, in the minority of cases, if deals do give rise to competition concerns in the UK, they may be subject to review by both the CMA and the EC. All things being equal, we would not expect an exit on a non-Norwegian model to result in a change in merger control policy or significant divergence between the EC and the CMA, at least in the short term. The CMA will
likely remain a member of several international competition law networks, the aim of which is to promote alignment of competition law application. However, if there were to be a more protectionist steer from the UK government post-Brexit, and if the current trends of increased UK government influence over the CMA’s activities continue, there is a possibility of divergence in the future.

There are two other potential developments to highlight if Brexit involved the UK falling outside the EU merger control regime. First, this may prompt the CMA to reconsider the nature of its own regime, and a potential move to a mandatory and suspensory model. Clearly, this would result in greater cost and complexity for private equity deals involving the UK. Secondly, there is a possibility that English may cease to be a working language of the EC. That would mean either that EC merger control notifications would require translation or that private equity firms may choose to use European lawyers with appropriate language skills.

Data Protection
The UK Data Protection Act 1998 (“DPA”) currently remains in force. All processing of personal data must be undertaken in accordance with the DPA, and the EU General Data Protection Regulation (“GDPR”) will be enforced within the EU from 25 May 2018. Organisations that provide goods and/or services in or to the EU are, for the most part, preparing for GDPR implementation and UK organisations should continue to do the same. Reform of UK data protection law remains necessary, but it is unclear whether the GDPR will be adopted in the UK.

Currently, the DPA allows for personal data to be transferred freely between member states and those countries covered by EC adequacy findings. The DPA also provides that consent, model clauses, binding corporate rules (“BCRs”) and self-assessed adequacy may be used to legitimise transfers of personal data outside the EU. The EU-US Privacy Shield was also adopted on 12 July 2016 as a means for legitimising data transfers to the USA.

What Is The Impact On Data Protection Under The Potential Future Options?
The future of UK data protection law will be influenced by the agreements that the UK reaches with the EU. Possible data scenarios are set out below.

- **Implement the GDPR (or an equivalent)**
  The UK may decide to implement the GDPR (or something very similar) and repeal the DPA. This should assist in the facilitation of continued trade links with the EU, and would likely result in an adequacy finding in the UK’s favour.

- **The Norwegian Model**
  Under a Norwegian Model, the UK would need to adhere to the GDPR from 25 May 2018, both before and after Brexit. Under this option, data transfers from the UK across the EEA would be permitted freely. The UK would likely also be able to continue to rely on any EC adequacy decisions in respect of non-EU countries, as well as the EU-US Privacy Shield decision.

- **The Adequacy Route**
  If the UK were to leave the EU and does not become part of the EEA, it would be treated as a third country by the EU for the purposes of international personal data transfers. If the UK retains the DPA and does not implement an equivalent to the GDPR, then it is likely that no finding of adequacy would be made in respect of the UK, as the GDPR is more robust in its protection and requirements than the DPA (the Investigatory Powers Bill also makes an adequacy decision even less likely). In this scenario, all personal data transfers to the UK from the EU would need to be legitimised by model clauses, BCRs, consent or any of the other safeguards or derogations available under the GDPR. This would likely require many organisations to review commercial contracts and data sharing arrangements that are currently in place to ensure ongoing compliance.

- **An EU-UK Privacy Shield?**
  If the UK decided to remain outside the EEA and no EC adequacy decision was made in respect of the UK, it might be possible to implement an EU-UK...
“privacy shield” type arrangement similar to the EU-US Privacy Shield.

**A Dual System?**

Finally, the DPA could remain in force and be applied to all international data flows from the UK outside the EEA when a controller is established in the UK, where the processing of personal data takes place exclusively in the UK and the processing is limited to UK citizens. For all other international transfers the GDPR would apply. Although this could assist small UK businesses, the complexity of administration makes this impractical.

It remains unclear which option the UK government will choose prior to May 2018. For most organisations, the prudent course of action based on the information available would be to continue with preparations for GDPR compliance.

**Intellectual Property**

On Brexit the UK intellectual property, ("IP") scheme (and to some extent the European IP scheme) is likely to become more complex. Harmonized EU IP laws may change in time, resulting in potential inconsistency. Individual IP rights are likely to be affected differently, with pan-EU rights, such as registered EU Community trade marks and designs, being more affected than national rights such as patents, copyrights and rights to prevent passing off/unfair competition. When Brexit occurs, unless specifically addressed in UK legislation, EU derived IP rights will no longer be recognised in the UK.

Consideration will also need to be given to the impact of cases that have been decided in accordance with prior EU judgments or decisions.

**Patents**

Until Brexit occurs, unless repealed, the Patents Act 1977 would remain in force regulating patents in the UK. In most cases, UK patents are nationalized versions of European patents granted by the European Patent Office ("EPO"). There would be no legal impact on the existing patent rights, as the EPO is independent of the EU. Brexit is also unlikely to affect the UK’s participation in the Patent Cooperation Treaty, the Paris Convention and the European Patent Convention, as these are all treaties outside of the EU.

However, Brexit may influence the UK’s introduction of the Unitary Patent Scheme and the Unified Patent Court ("UPC"), which are due to take effect in 2017—although ratification of the agreement is still legally possible.

Brexit will likely delay and potentially impair the introduction of the UPC throughout Europe. Before the UPC can start, it must be ratified by at least 13 member states, including the UK. The UPC thus cannot start anywhere in Europe while the UK remains an EU member but has not ratified the UPC, unless the UPC agreement were to be renegotiated to remove the UK ratification requirement.

**Trade Marks**

Following Brexit the Trade Marks Act 1994 (unless repealed) would remain in force for the regulation of registered trade marks in the UK. The UK would no longer be part of the EU Trade Mark ("EUTM") system, as it is only accessible to member states. This would undermine the enforceability in the UK of existing European Trade Mark registrations. It is possible that a conversion process will be needed to convert EU Trade Marks to UK National Trade Marks and ensure the continuity of rights. Until then, all EU Trade Marks registered or awaiting registration will continue to benefit from protection within the UK and other member states.

**EU Design Rights**

Registered EU Community design rights cover all member states and further legislation will be expected in order to preserve them. The UK may allow all existing EU designs to apply and later allow conversion into UK designs.

**Copyrights**

Copyright protection is not fully harmonized in the EU and is mostly based on domestic law. It is unlikely that Brexit will impact significantly on UK copyright.

**Database Rights**

Database rights are protected in the UK under the Copyright and Rights in Databases Regulations 1997.
Like copyright, such rights are automatic and Brexit is unlikely to affect their formalities or protections. However, the Regulations refer to an individual or a body incorporated in an EEA state in order for the database right to be qualified, which would, perhaps, require amendment.

Conclusion

Given the uncertainty surrounding Brexit, the long term impact on IP rights in the UK is still unclear. The UK government will have to work closely with the EU in the future to fill the gaps in the areas of EU trade marks and design rights and, possibly, in unitary patents and the UPC. The UK Government will likely delegate the responsibility for scoping the new IP landscape to the UK Intellectual Property Office and the increase in its administrative function may result in increased filing costs for those registering or renewing IP rights in the UK.

Government Enforcement/White Collar Crime

EU influence over criminal law and criminal justice is exercised in five general areas:

- **Substantive criminal law** legal instruments such as Directives and Regulations intended to harmonise the development of the substantive criminal law in areas such as money laundering and people trafficking;

- **Criminal procedure** measures intended to influence national criminal procedure such as those concerning the standing of victims in criminal proceedings and the rights of defendants;

- **Police cooperation** measures intended to enhance police cooperation such as sharing of fingerprint and DNA information;

- **Mutual recognition** measures intended to enhance the recognition of criminal decisions and warrants between member states, such as the European Arrest Warrant and mutual assistance in freezing assets; and

- **EU policing agencies** Europol (which plays a coordination and intelligence role between the policing agencies of member states) and Eurojust (which plays a coordination role for prosecutors).

Prior to the Referendum the UK had opted in to a small number of EU criminal law measures (such as child sexual abuse and human trafficking) and a handful of measures relating to the rights of suspects. It seems unlikely that these measures will be reversed in the UK on Brexit.

Most EU law in the field of criminal justice (since the Lisbon Treaty in 2009) has been enacted via EU Directives that are then implemented in the UK by way of secondary legislation. Noteworthy among these Directives is the forthcoming 4th Money Laundering Directive (“4MLD”). There are, at the time of writing, proposals for the implementation date of 4MLD to be brought forward to early 2017 in response to the increase in terror-related attacks in Europe. Whether these proposals are adopted or not, the UK will be required to give effect to 4MLD well before the UK has formally left the EU. Moreover it seems unlikely that the UK will want to undo the effects of 4MLD as many of the changes contained in 4MLD come themselves from Financial Action Task Force recommendations.

Following Brexit it remains to be seen how the UK might adopt or follow criminal laws originating in the EU. It seems unlikely that the UK will want to withdraw completely from areas such as cross border policing cooperation. It also seems unlikely that any significant consequences would follow from the UK’s ceasing to be bound by the EU instruments designed to harmonise aspects of substantive criminal law or procedure such as cybercrime or people-trafficking.
November 2, 2016

An Update on Brexit and the Implications for General Data Protection Regulation (GDPR)

Following the “Leave” result of the United Kingdom’s referendum on its membership in the European Union, there has been uncertainty regarding the implementation of the General Data Protection Regulation (GDPR) due to come into effect on 25 May 2018. Our report on the GDPR explains the key changes to Data Protection Law.

On 24 October 2016, the Secretary of State for Culture, Media and Sport, Karen Bradley MP, confirmed that the UK will still be in the EU in 2018 and will be opting-in to the GDPR. As a result, businesses collecting or using personal data while providing goods or services in the EU of EU data subjects will be subject to the new regulations.

The UK’s data protection authority, The Information Commissioner’s Office, supports this stance taken by the government and has confirmed it will issue a statement in the next month setting out a timeline for publishing its guidance on the GDPR in the upcoming months.

Both the ICO and UK government have reiterated the necessity of complying with the GDPR. In light of the increased scope of fines for non-compliance with the GDPR, it is imperative that businesses assess the steps they need to take to ensure compliance by May 2018.

For more information regarding the GDPR and its potential impact, please contact Ropes & Gray’s leading privacy & data security team.
02 February 2017

**BREXIT WHITE PAPER PUBLISHED**

Earlier today, the UK government published an official policy paper (the White Paper) setting out the government’s approach to leaving the European Union (EU). The publication of the White Paper follows the House of Commons vote yesterday in favour of the European Union (Notification of Withdrawal) Bill, which provided Theresa May with the authorization needed to invoke Article 50 in order for the UK to leave the EU.

Building on last week’s speech by the Prime Minister on the government’s plan for Brexit, the White Paper sets out once again the 12 principles that will guide the government during its negotiations with the EU. The White Paper sets out the government’s basis for each of the 12 principles and the broader strategy underlying them. From the perspective of financial services, rather than providing new material information, key themes from Theresa May’s speech are reiterated.

The Principles are as follows:

1. Providing certainty and clarity.
2. Taking control of the UK’s laws.
3. Strengthening the Union.
4. Protecting our strong historic ties with Ireland and maintaining the Common Travel Area.
5. Controlling immigration.
6. Securing rights for EU nationals in the UK and UK nationals in the EU.
7. Protecting workers’ rights.
8. Ensuring free trade with European markets.
9. Securing new trade agreements with other countries.
10. Ensuring the UK remains the best place for science and innovation.
11. Cooperating in the fight against crime and terrorism.
12. Delivering a smooth, orderly exit from the EU.

**The Great Repeal Bill**

With respect to the first and second principles, the White Paper confirms the Government’s intention to introduce a “Great Repeal Bill” to remove the European Communities Act 1972 and to preserve EU law. All EU laws which are directly applicable in the UK (such as EU regulations) and all laws which have been made in the UK to implement the UK’s obligations as a member of the EU will be “preserved” – and so will remain part of domestic law on the day the UK leaves the EU. The White Paper also confirms that the preserved law will continue to be interpreted in the same manner as currently – whether this will be workable remains to be seen.

Parliament will also determine the content of other primary legislation if there are any significant policy changes. The Government expects to introduce separate bills on immigration and customs, and there will be a programme of secondary legislation under the Great Repeal Bill to address so-called “deficiencies” in the preserved law, the details of which are not provided. The government will eventually publish a White Paper.
on the Great Repeal Bill. As we have highlighted in our previous alerts, the introduction of the Great Repeal Bill will no doubt result in a number of complex discussions, and analysis will be required for a smooth transition of such a vast body of law, regulation and guidance.

**Withdrawal from Single Market Access**

In connection with Principle 8 (Ensuring free trade with European markets), the White Paper reiterates the Government’s position that it will not seek membership of the EU Single Market but will instead pursue a new strategic partnership with the EU, including a Free Trade Agreement and a new customs agreement. As outlined in Theresa May’s speech last week, the agreement may well reflect elements of the existing Single Market arrangements. No further details of the agreement are provided in the White Paper.

With respect to the provision of financial services across the European Union, the White Paper does not provide any additional information to that which was provided in Theresa May’s speech. The White Paper confirms that the aim of the government is for the “freest possible trade in financial services between the UK and EU Member States”. This is clearly a “watch this space” element of future negotiations, much of which we have discussed in previous alerts on the implications of Brexit on financial services: Click Alerts.

For The United Kingdom’s exit from, and new partnership with, the European Union White Paper, click Here.

For more detailed analysis of the issues, please contact your usual Ropes & Gray partner. For additional Brexit resources, please refer to the Ropes & Gray Brexit webpage.
If you have any questions on this Alert or Brexit-related queries, then please contact your usual Ropes & Gray contact or reach out to our UK Asset Management team.
August 31, 2016

China FDA Clarifies Legal Consequences of Clinical Trial Data Inspections

China’s recent drug regulatory reform has emphasized that clinical trial data must be authentic and reliable. However, the legal consequences for breaching data integrity requirements in clinical trials remain ambiguous. On August 24, 2016, the China FDA (“CFDA”) issued a draft Guideline for Handling Issues Identified in Clinical Trial Data Inspections (“Draft Guideline”). The Draft Guideline aims to clarify what constitutes data forgery and the legal consequences of noncompliance in clinical trials for different stakeholders. The CFDA is currently seeking public comments on the Draft Guideline.

Previously, the CFDA issued on July 22, 2015, a circular requiring all applicants of 1,622 pending drug registration applications to self-inspect their clinical trial data and compliance with the Good Clinical Practices (GCP). The circular highlighted several priority areas for the self-inspection, such as consistency of the final data for analysis with the original raw data, documentation of changes, compliance in handling of samples and investigational products, management of subject screening, inclusion and exclusion, keeping track of protocol deviations and reporting of adverse events. Upon self-inspection, applicants voluntarily withdrew around 80% of the pending applications, including domestic and imported drug applications. Based on the submitted self-inspection results, since early 2016 the CFDA has initiated five rounds of onsite inspections over selected clinical trials, including some Phase I to III trials and some BE studies. Among the first three batches of completed inspections, 30 drug applications were rejected, in most instances based on findings of false clinical data.

To provide more guidance on the legal consequences of these CFDA-led inspections, the newly issued Draft Guideline mainly addresses the following:

- **Division of liability between applicants/sponsors, clinical trial institutions/sites, and clinical research organizations (CROs).** While sites and CROs shall bear liability for those data integrity issues, they are directly responsible for, the sponsors ultimately bear all the legal liabilities for the submitted clinical data and drug application dossier.

- **Types of GCP breaches that constitute data forgery.** The Draft Guideline gave a specific list of violations of relevant sections of GCP that constitute data forgery. Among others, hiding certain trial data or not presenting the complete data set is considered data forgery, which can lead to CFDA’s ban on the applicant’s future applications (see the bullet below).

- **Ban on future applications.** Companies that have forged clinical trial data are banned from refiling an application for the same product with the CFDA for the next three years. In particular, if data forgery is found to have occurred after November 11, 2015, the CFDA will directly reject the current application under review, and the applicant will be banned from filing any applications for any drug products for one year.

- **Implementing a blacklist.** Based on the Draft Guideline, blacklisting will apply not only to the sponsors, sites and CROs involved in data forgery, but also to the responsible individuals within these entities.
- **Suspension of studies at study sites.** If study sites are found to be involved in data forgery, or to have committed other serious GCP violations that threaten subject safety or data integrity, the sites must immediately suspend subject enrollment, rectify the misbehavior, and refrain from undertaking any new trials.

- **Discretion in imposing penalties.** Applicants can be exempted from penalties if they voluntarily report all identified issues through self-inspection and withdraw the questionable applications. There will be leniency in penalties if applicants fully cooperate with the investigation and timely explain and correct the identified noncompliance. On the other hand, applicants who decline, deter, or avoid inspections can face higher penalties.

We encourage life sciences companies to arrange necessary audits of ongoing clinical trials, evaluate the level of GCP compliance, and develop corrective action plans accordingly.

If you would like to discuss the foregoing or any other related matter, please contact Katherine Wang or your usual Ropes & Gray advisor.
Donations and Grants in China: Compliance Controls Beyond T&E

While travel and entertainment expenses have presented significant compliance challenges for life sciences companies operating in China, donations and grants can also pose notable compliance risks. China’s escalated anti-corruption enforcement in recent years is well-publicized, and regulators have taken interest in grants and donations in the life sciences space. For example, in early 2015, the State Administration of Industry and Commerce (“SAIC”), which enforces commercial bribery regulations, published specific guidance on this issue for the pharmaceutical industry. More recently, the National Health and Family Planning Commission (“NHFPC”), China’s regulator for the health care services sector, also enacted specific measures on donations for health care-related organizations. These trends suggest potential scrutiny from enforcement officials towards grants and donations, which may be areas that deserve additional attention from legal and compliance professionals in the life sciences sector.

I. New NHFPC Regulations on Donations

On October 20, 2015, the NHFPC published Measures for Administering the Receipt of Public Welfare Donations by Health and Family Planning Organizations (“New Measures”). Despite being announced in October, the New Measures became effective as of August 26, 2015, and replaced the previous measures enacted in 2007, entitled Interim Measures for the Administration of the Acceptance of Social Donations and Financial Aid by Health care and Health Institutions (“Old Measures”).

The New Measures apply to donations received by hospitals, health care institutions and other health care organizations (e.g., medical associations, funds and charities) overseen by the NHFPC, regardless of whether the donations are made by domestic or foreign life sciences companies. The types of donations subject to the New Measures include funds and tangible property, though they are not necessarily exclusive. In particular, the New Measures provide detailed guidance on what donations would be considered appropriate, in part by expressly listing acceptable purposes for donations and prohibited types of donations. Additionally, the New Measures further require that health care institutions establish appropriate controls and procedures in accepting donations.

Although the New Measures technically apply to health and family planning institutions and organizations receiving donations, the detailed guidelines may indirectly impact how life sciences companies provide donations to those organizations and institutions. In turn, life sciences companies, both foreign and domestic, may want to ensure that their internal controls are consistent with the requirements of the New Measures.

Permitted and Prohibited Donations

Unlike the Old Measures, the New Measures expressly enumerate the types of donations that recipients are permitted to accept, which include donations for public health care education, training health care professionals, academic activities and research studies, discounting or waiving costs for medical treatments, and other non-profit programs. At the same time, it expressly prohibits acceptance of certain categories of donations, which include donations related to profit-seeking commercial activities, donations related to the procurement or purchase of products or services, donations where the donor has an interest in the economic benefits, intellectual property rights, research results or industry data of said donation, and donations that do not conform to laws and regulations or involve potential unfair competition and commercial bribery.
Interestingly, the prohibition against commercial bribery appears to create a link to the SAIC and local AICs. As noted above, while the New Measures apply directly to health care-related institutions, its list of expressly permitted and prohibited donations could potentially affect the AIC’s interpretation in its commercial bribery enforcement actions.1

Procedural Requirements

The New Measures also set forth certain procedural requirements for donations, many of which are expansions of the Old Measures. For example, donations must still be documented via a written agreement, but the New Measures expressly require that certain information be specified, such as the type, quantity, quality and value of the donated items, the intention and purposes of the donation, restrictions on the management and use of the donated items, etc. The New Measures further provide clear requirements on the method of making donations, including, among other things, that monetary donations be made via bank transfers and that donations in the form of tangible property (e.g., products or equipment) undergo fair market valuation, preferably by a third-party appraiser.

The New Measures also appear to take a further step in requiring transparency. A donation recipient is required to publicize its written policies on accepting donations and disclose donations it has accepted, including the nature of the donated item, the value of such item, and how the item is used, on its website or via mainstream news media. Donation recipients must also report accepted donations in its annual financial statements, along with detailed explanations. Moreover, donation recipients are required to answer public inquiries about donations that they have accepted.

Notable Provisions that Require Further Clarification

The New Measures contain two provisions that are unclear, but may have particular relevance to life sciences companies in China. The first is a requirement that donations for training health care professionals, academic activities or scientific research may not designate the specific recipient or beneficiary. It is unclear, however, whether the scope of this restriction includes company sponsorships of specific health care professions (“HCPs”) to attend academic meetings or professional trainings, or sponsorship of a particular principal investigator in conducting certain medical studies or clinical trials. The second requirement is an express prohibition against donations related to “profit-seeking commercial activities,” which is not further defined. It is unclear whether this provision could be interpreted broadly to preclude donors from allowing display booths, spaces or other product promotion or marketing presence at an event.

Since its announcement, there has been little public information about enforcement actions pursuant to the New Measures, so it remains to be seen how the NHFPC will interpret these provisions. Nonetheless, some local hospitals and NHFPC-regulated entities have made public announcements stating that they will update their donation policies to comply with the New Measures.2 For the time being, however, life sciences companies should pay close attention to further guidance or enforcement signals from the NHFPC and AIC with respect to donations and grants.

---

1 As of the time of this article, the AIC has not published any cases instructive to this point and it remains unclear how the New Measures will influence AIC enforcement behavior.

2 On January 10, 2016, Peking University People’s Hospital implemented a local policy regarding administering the receipt of non-profit donations, based on the New Measures. Similarly, on February 18, 2016, Chongqing Cancer Hospital implemented a local policy regarding administering the receipt of non-profit donations, based on the New Measures. On May 10, 2016, Tianjin Health and family Planning Commission announced on its website that the local districts/counties and hospitals should follow the New Measures.
II. Compliance Controls and Monitoring in Relation to Donations and Grants

While the ultimate impact of the New Measures is yet unclear, the underlying compliance risks nonetheless warrant attention. In recent years, pharmaceutical and medical devices companies have made significant efforts to enhance compliance controls and monitoring around travel and entertainment expenses. However, donations and grants are not devoid of FCPA risks and they can present unique compliance challenges. The most significant of those risks stem from involvement of a third party, which means limited control and transparency. In response, similar controls and monitoring for third parties should be undertaken, some of which include:

- **Ensure Clear Policies and Protocols**

  While most companies’ general anti-corruption and anti-bribery policies include provisions related to donations and grants, special attention to these issues may be warranted. For example, shielding involvement of sales and marketing functions from the company’s internal decision-making process, particularly with respect to selecting recipients, can minimize potential *quid pro quo* considerations that may influence the decision (or the optics thereof). In fact, companies may want to limit the extent to which it designates eventual use of the donated funds or items to particular HCPs who would derive a benefit therefrom. Decisions on donations and grants often involve business considerations, and clear protocols can ensure that those decisions are subject to compliance controls.

- **Perform Due Diligence on the Recipient and Third-Party Intermediaries**

  Due diligence should focus on uncovering any governmental relationships and assessing the reputation and appropriateness of the recipient or donee. Bribery risks can arise where the donation may be deemed to indirectly benefit a government official linked to the recipient organization. For example, if due diligence uncovers that the recipient is an organization established by an influential government official whose position or office happens to be relevant to the company’s business, the company may wish to balance the potential risks and/or take additional steps to assess the appropriateness of the donation and implement enhanced compliance safeguards.

  Also, recipients, such as hospitals, medical associations and charitable organizations, are not impervious to fraud and misappropriation, as exemplified in accusations against the Red Cross Society of China regarding donations to aid victims of the devastating 2008 Sichuan earthquake.3 There may be additional reputational risks with providing donations to a recipient that is linked with improprieties and accusations of misconduct.

  Finally, employees might collude with the recipient or third-party intermediaries to engage in misconduct. Best practices would involve performing due diligence on any third-party intermediaries that are involved. Additionally, it may be worthwhile to understand the level of compliance controls employed by the intermediary to assess third-party compliance risks.

- **Ensure Appropriate Terms and Safeguards are Included in Donation, Grant, or Sponsorships Agreements**

  The New Measures already require that the written donation agreements set out detailed terms of the donation. Accordingly, compliance terms should also be included. Such terms can set forth appropriate anti-bribery representations and warranties, a covenant from the recipient that the donated funds or items will only be used in accordance with the stipulated purpose and will not be reassigned or transferred, an obligation to provide any required supporting documents and information to show how the funds are actually

3 See [here](#) and [here](#).
used, and audit rights (to the extent practicable), among other provisions. Also, it is not uncommon in China for donation or grant recipients to informally solicit suggestions from company employees on the use of funds, including any preferences on selecting HCPs who may benefit from the donation, which can increase bribery risk. Hence, companies may also wish to clearly stipulate the company’s detachment and independence from the use of the funds.

- **Post-Donation Monitoring and Verifications**

  Similar to travel and entertainment expenses, securing supporting documentation and conducting follow-up verification are important steps towards detecting and deterring misappropriation and fraud in the context of donations and grants. Because third parties are involved, detailed supporting documentation and information tend to be more challenging to obtain. As noted above, companies may wish to establish controls and protocols for follow-up verifications and include contractual obligations for the recipient and/or intermediary to provide necessary supporting documentation and information in the written agreement.

Given the recent regulatory attention to donations and grants, particularly within China’s heightened anti-bribery enforcement climate, compliance professionals in the life sciences sector may wish to pay particular attention to how donations and grants are being provided and enhance their compliance programs, where needed, to reduce compliance risks related to donations and grants.
November 16, 2016

Recent Developments in Japanese Enforcement of Foreign Bribery Laws

In recent years, Japan has been under increasing scrutiny and pressure from the international community regarding its enforcement of its anti-corruption laws. A signatory to the OECD Anti-Bribery Convention, Japan enacted an amendment to its Unfair Competition Prevention Law (“UCPL”), which came into force on February 15, 1999, to address bribery of foreign public officials. But the OECD Working Group on Bribery in International Transactions has continually criticized Japan for its relatively lax enforcement of anti-corruption. Indeed, while the UCPL is broad in scope and prohibits offering or giving any benefit to a foreign public official, Japan is reported to have prosecuted only four cases of bribery since 1999. In February 2014, the OECD Working Group expressed significant concerns about the lack of foreign bribery enforcement in Japan, noting that numerous allegations involving Japanese companies had been reported in the media, yet did not seem to have been prosecuted. Most recently, in June 2016, a high-level OECD mission met with government representatives and senior officials in Japan to urge them to take additional steps in furtherance of the OECD Anti-Bribery Convention.

Perhaps in response to the OECD’s criticisms, the Ministry of Economy, Trade, and Industry (“METI”) and the Japan Federation of Bar Associations (“JFBA”) have issued guidance in an effort to heighten awareness of anti-bribery issues and highlight the factors that Japanese regulators and foreign regulators will likely scrutinize. This guidance, issued in 2015 and 2016, indicates that anti-corruption is no longer an issue that companies in Japan should take lightly.

I. METI Guidelines Regarding Foreign Bribery

On July 30, 2015, METI revised its Guidelines for the Prevention of Bribery of Foreign Public Officials (“Guidelines”). The Guidelines, which were promulgated in 2004 and previously revised in 2010, had been criticized for being vague and abstract. The revision was published to clarify legal interpretations regarding conducting business internationally, with the purpose of supporting Japanese companies’ expansion overseas.

Although the Guidelines are not legally binding, they provide guidance on how Japanese anti-bribery law should be interpreted. The revision clarified that Japanese companies must reject demands for bribes from foreign public officials even if the bribes are made to avoid unreasonable and discriminatory treatment by those officials. On the other hand, the Guidelines clarified that small congratulatory gifts and travel and entertainment expenses may not be considered bribery if given solely to build a general social relationship or acquaint the official with the company’s products or services, rather than to demand advantageous treatment. Specific examples of acceptable gifts and hospitality include promotional giveaways or commemorative gifts for general distribution, refreshments at business meetings, and seasonal gifts of low value given in accordance with local custom and law.

One focus of the revised Guidelines was to enumerate anti-corruption best practices for Japanese companies conducting business overseas. Japanese companies were encouraged to adopt an internal control system to prevent foreign bribery, taking an approach tailored to the risks in each country and market in which they operated. They were also urged to pay close attention to the internal control systems at foreign subsidiaries, which may have difficulty managing their anti-corruption risks without the parent company’s support. The revised Guidelines also emphasized the importance of conducting review or diligence prior to taking risky operational decisions, such as the
hiring of local agents or consultants, selection of a joint venture partner, acquisition of a company, and participation in public procurement.

II. JFBA Guidance Regarding Anti-Bribery Measures

On July 15, 2016, the JFBA issued new guidance for companies regarding compliance with Japanese and foreign anti-bribery laws, called the Guidance on Prevention of Foreign Bribery (“Guidance”). The JFBA Guidance, which was intended to supplement the METI Guidelines, was published with the purpose of providing practical advice for Japanese companies and legal counsel seeking to implement anti-bribery measures. Its recommendations take into account both Japanese law and foreign bribery laws such as the Foreign Corrupt Practices Act and 2010 U.K. Bribery Act, and are meant to address both bribery of public officials and commercial bribery.

The Guidance echoed many of the messages in the METI Guidelines, including the importance of a comprehensive system of internal controls, monitoring, and training. The Guidance also emphasized the importance of managing third-party relationships by conducting risk-based due diligence and adopting contractual safeguards to mitigate risk. Notably, the Guidance encouraged management at Japanese companies to issue a declaration that they were adopting measures in accordance with the Guidance, with the expectation that this would lead to increased public confidence in the companies.

III. Implications of METI and JFBA Guidance

Companies conducting business in Japan, as well as Japanese companies conducting business overseas, should prepare for increased scrutiny from Japanese regulators in the coming years. When announcing the revision to the Guidelines, METI cited the expansion of Japanese companies to overseas marketing, including the infrastructure sector, as one of the factors that led to the revisions. A recent Japanese prosecution targeted this exact sector, and investigated allegations of bribes paid by Japan Transportation Consultants, Inc. to foreign officials in Vietnam, Indonesia, and Uzbekistan in a bid to gain railway projects. Increased anti-corruption enforcement globally in the life sciences sector may lead to closer attention by Japanese regulators to medical and pharmaceutical companies.

Japan will next be evaluated by the OECD Working Group in March 2019, which may lead to additional enforcement. The OECD Working Group has repeatedly urged Japan to adopt two additional enforcement efforts. The first is amending Japan’s Anti-Organized Crime Law, rendering it impossible for companies and individuals convicted of bribing foreign public officials to keep their illegal proceeds, including by laundering them. The second is to adopt an action plan to organize policy and prosecution resources to be able to proactively detect, investigate, and prosecute cases of foreign bribery involving Japanese companies.

In the face of increased scrutiny, companies with operations or headquarters in Japan are advised to evaluate their internal system of controls to ensure compliance with international anti-corruption compliance standards.
December 20, 2016

China Solicits Comments on Drug GCP

The China Food and Drug Administration (“CFDA”) recently proposed revisions to the Good Clinical Practices for Pharmaceuticals (“GCP”), the most comprehensive revision in 13 years. The revisions (“Revisions”) are now open to public comments until January 31, 2017.

It’s notable that the Revisions have rewritten all the articles of the current GCP, but these sweeping changes are not especially innovative, as most of the concepts and principles have already been addressed in the International Conference on Harmonisation (“ICH”) GCP.

Overall, the Revisions set forth general principles of conducting clinical studies in China, as well as guidance of roles and responsibilities for the ethics committee (“EC”), the investigator and the sponsor, as well as the requirements for protocol and investigator’s brochure (“IB”). Highlights of the changes proposed in the Revisions are as follows:

- **Regulate the Handling and Retention of Biological Specimens:** According to the Revisions, the sponsor shall be prohibited from conducting any testing that is unrelated to the study protocol approved by the EC on biological specimens. Additionally, the Revisions would require the sponsor to seek written consent from the subjects regarding the continuous storage of and/or possible use in any future research of leftover biological specimens after completion of the trial. The consent form would have to specify issues such as the retention period, the data confidentiality requirements, and the circumstances under which the data and specimens could be shared with other investigators.

- **Extend Insurance Coverage to Institutions:** Unlike the current GCP, the Revisions would require the sponsor to insure or indemnify both the investigator and the institution against all claims, except for those arising from malpractice.

- **Allow an Individual to Serve as Sponsor or CRO:** As a response to the pilot program of marketing authorization holder promulgated by the State Council this past June, the Revisions would allow individuals to act as sponsors and contract research organizations (“CROs”).

- **Specify the Requirement and Quantity of Retention Samples:** Under the Revisions, reserve samples of study drugs for bioequivalence and bioavailability testing must be retained at the study site for no less than two years after marketing approval. The investigator will randomly select the reserve samples from the supply sent by the sponsor and should retain enough to allow five rounds of quality standard testing.

- **Detail the Process of Seeking Informed Consent from Subjects:** Under the Revisions, the EC would have to pre-approve any new information that may affect subjects’ willingness to participate in the study. Importantly, the Revisions would prohibit agreements (whether oral or written) that ask subjects to waive their legal rights, or that may release the investigator, the institution, the sponsor, or its agents from liability.

- **Add Notification Requirement of the Unblinding Results:** The Revisions propose that, for any double-blinding studies, the sponsor must provide the investigator and all study participants with the treatment allocation status after unblinding.
• **Revise the Data Retention Requirement:** Whilst the current GCP imposes different data retention requirements on the investigator (e.g., five years after the study ends) and the sponsor (e.g., five years after obtaining marketing approval), the Revisions would impose similar obligations on both: data would have to be retained for two years after marketing approval or for five years after the study ends.

• **Require to Specify Direct Access to Source Records:** The Revisions would require that under either the protocol or the clinical trial agreement ("CTA"), the investigator and the institution must be required to give the monitors and auditors direct access to the source data and source documents related to the clinical trial. This change may help clarify the industry’s concern regarding who may have access to subjects’ medical records to verify the authenticity of the study data, especially for the clinical trial data inspection campaign.

• **Clarify Contractual Arrangements Regarding CTA:** The Revisions clearly stipulate that a CTA shall be structured as a three-party agreement between the sponsor, the investigator and the institution. Each party shall sign the CTA on his/her own capacity. In addition, for multi-center trials, the Revisions specify that the sponsor shall sign the CTA with all participating investigators and the relevant institutions.

• **Impose Regular Review Requirement of IB:** The requirement regarding the IB in the current GCP is simple and general. The Revisions would incorporate the same detailed regulatory requirement on IB as that provided in the ICH GCP. In particular, according to the Revisions the sponsor must establish a written procedure regarding amendments to the IB, noting that the IB needs to undergo a review and amendment at least once per year. In addition, the Revisions add several provisions to set forth the purpose, general considerations, and contents regarding the IB.

• **Adopt Some Changes Reflected in the Latest ICH GCP:** The latest version of the ICH GCP, the E6 (R2), was adopted by the ICH on November 9, 2016. Accordingly, the Revisions include a number of the new changes reflected in the E6 (R2), such as the notions of certified copies and validation of computerized systems, as well as the sections regarding quality management, risk management, oversight of CROs, and risk-based monitoring, among others. To some extent, it reflects CFDA’s willingness to establish a regulatory framework in line with international standards.

The Revisions would standardize the conduct of drug studies in China, as well as strengthen the management of such studies. It remains unclear whether and when these changes will be adopted. We recommend that pharmaceutical companies closely monitor the progress of the Revisions and propose their comments by the deadline.

If you would like to discuss the foregoing or any other related matter, please contact Katherine Wang or your usual Ropes & Gray advisor.
CFDA Amends Medical Device Recall Rules

Recently China’s Food and Drug Administration (“CFDA”) released the Provisions for Medical Device Recall (“New Recall Rules”). The New Recall Rules, becoming effective on May 1, 2017, will replace the existing Interim Provisions for Medical Device Recall promulgated by the former Ministry of Health in 2011 (“Existing Recall Rules”). The New Recall Rules follow the basic regulatory framework for device recall provided in the Existing Recall Rules. Recalls are divided into mandatory recalls (imposed by local FDAs) and voluntary recalls (initiated by device manufacturers). Depending on the severity of product defects, recalls are classified as Level 1 recalls (products caused or may cause serious damage to health), Level 2 recalls (products caused or may cause non-lasting or reversible damage to health) or Level 3 recalls (products carry only a minor risk of causing damage to health). Under these different recall scenarios, device manufacturers are further subject to different requirements for recall implementation. Device distributors and device-using hospitals are also obligated to cooperate with or assist the manufacturers during the recalls. Compared with the Existing Recall Rules, the New Recall Rules introduced the following major changes:

Clarity on application scope and responsible entities for recall

The New Recall Rules apply to the recall of medical devices marketed in China. For domestic products, the holder of the product’s registration license is responsible for recall; for imported products, the designated regulatory agent of the foreign device manufacturer in China is responsible for recall. If a foreign manufacturer initiates a recall outside China for a product also marketed in China, its local agent must timely report the recall-related information to the CFDA.

Expand the scope of Defective Products

In the Existing Recall Rules, Defective Products (i.e., products that should be recalled) are defined as devices that pose unreasonable risk of potentially damaging human health or life safety when used under normal conditions. The New Recall Rules enlarge the existing definition by adding three more types of Defective Products: (a) products that do not conform to compulsory standards, or to the product’s technical specifications registered or filed with the CFDA; (b) products that pose unreasonable risk due to the failure to comply with the applicable quality management rules for device manufacture and supply; and (c) products that for other reasons must be recalled.

More severe penalties for manufacturers that refuse to implement mandatory recalls

Local FDAs may identify, investigate and assess devices with potential defects and determine upon their own discretion that such products should be recalled. In the event of such mandatory recalls, if device manufacturers refuse to implement the recalls, the Existing Recall Rules allow the local FDAs to impose monetary fines of three times the total value of products that should be recalled. The New Recall Rules, on the other hand, refer to the penalty provisions under Article 66 of the State Council’s Regulation for the Supervision and Administration of Medical Devices (Order 650), which allow the local FDAs to impose fines of up to ten times the goods’ value.

The Provisions for Medical Device Recall form an important part of China’s new device regulatory regime centering around Order 650. Device companies with product sales or local operations in China are recommended to review the New Recall Rules and keep their post-market product safety measures in line with the more stringent regulatory requirements.

If you would like to discuss the foregoing or any other related matter, please contact Katherine Wang or your usual Ropes & Gray advisor.
February 16, 2017

Hong Kong Proposes Enhanced AML Obligations for Professionals and Beneficial Owner Registries for Hong Kong Companies

The Hong Kong Government has recently proposed to expand its anti-money laundering (“AML”) laws. This is expected to assist Hong Kong in keeping pace with AML developments in other financial centers, and to prepare for its upcoming FATF mutual evaluation in 2018.1

Key Proposals

- Hong Kong companies would be required to maintain a register of “beneficial owners” or “persons with significant control,” known as a PSC register.

- Solicitors, accountants, real estate agents, and trust or company service providers would be required to perform customer due diligence in certain circumstances.

Beneficial Owner Registers

The government proposes to amend the Companies Ordinance to require Hong Kong companies to identify and maintain records of their “beneficial owners.” The definition of “beneficial owners” would also be significantly revised. These proposed rules would apply to all companies incorporated in Hong Kong, including companies limited by shares, companies limited by guarantee and unlimited companies. However, listed companies will be exempt given the existing regime already imposed on them under the Securities and Futures Ordinance (Chapter 571 of the Laws of Hong Kong).

If approved, such companies will be required to create a “PSC Register” of persons with “significant control.” Persons with “significant control” include both registrable individuals and registrable legal entities. This register would be available for public inspection on payment of a fee.

“Registrable individuals” are beneficial owners, as that term is newly defined under the proposed amendments. Historically, a “beneficial owner” was defined as an individual who owns or controls, directly or indirectly, not less than 10% of the issued share capital of the corporation, or who is, directly or indirectly, entitled to exercise or control the exercise of not less than 10% of the voting rights at general meetings of the corporation, or who exercises ultimate control over the management of the corporation.

Under the proposed amendments, “beneficial owners” would be individuals who meet one or more of the following specified conditions:

- Directly or indirectly holding more than 25% of shares;

---

1 Hong Kong Financial Services and the Treasury Bureau, Consultation on Enhancing Anti-Money Laundering Regulation of Designated Non-Financial Businesses and Professions, available here; and Hong Kong Financial Services and the Treasury Bureau, Consultation on Enhancing Transparency of Beneficial Ownership of Hong Kong Companies, available here.
• Directly or indirectly holding more than 25% of voting rights;

• Directly or indirectly holding the right to appoint or remove a majority of directors;

• Otherwise having the right to exercise, or actually exercising, significant influence or control; or

• Having the right to exercise, or actually exercising, significant influence or control over the activities of a trust or a firm that is not a legal person, but whose trustees or members satisfy any of the first four conditions (in their capacity as such) in relation to the company, or would do so if they were individuals.

In its consultation paper, the government stated that they might “take this opportunity to align the threshold under the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (the “AMLO”) with the proposed 25% threshold to be adopted under the Companies Ordinance.” Accordingly, this revision would likely also apply to financial institutions that are currently subject to AML customer due diligence requirements.

“Registrable Legal Entities,” in turn, are defined as any legal entity immediately above the company in its ownership chain that meets the beneficial ownership definition.

Companies would be required to obtain and ascertain the accuracy of the following information required to be included in the PSC register: the beneficial owner’s name; his or her or its identity card or passport details, or company registration number; his or her or its address; the date he or she or it became a registrable individual or entity; and the nature of the control exerted over the company. If there is no person or entity that falls within the definition of registrable individual or legal entity, the new rules would also require that this be stated in the PSC register. Registrable individuals and entities would be required to comply with notices to ascertain and confirm the relevant particulars.

Customer Due Diligence and Recordkeeping Obligations for Solicitors, Accountants, Real Estate Agents and Trust and Company Service Providers.

A proposed amendment to the AMLO would extend customer due diligence (“CDD”) recordkeeping requirements to three types of professions performing specified kinds of roles:

• **Solicitors and accountants**, when preparing for or carrying out transactions for clients concerning

  i. the buying or selling of real estate;

  ii. managing of client money, securities or other assets;

  iii. management of bank, savings or securities accounts;

  iv. organization of contributions for the creation, operation or management of companies;

  v. creation, operation or management of legal persons or arrangements; or

  vi. buying or selling of business entities;

• **Real estate agents**, when engaged in transactions concerning the buying and selling of real estate; and

---

2 See Hong Kong Financial Services and the Treasury Bureau, Consultation on Enhancing Anti-Money Laundering Regulation of Designated Non-Financial Businesses and Professions, p.19, available [here](#).
**Trust or Company Service Providers (“TCSPs”),** when preparing for or carrying out transactions for clients concerning

i. the forming of companies or other legal persons;

ii. acting, or arranging for another person to act, as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;

iii. providing a registered office, business address, correspondence or administrative address or other related services for a company, a partnership or any other legal person or arrangement; or

iv. acting, or arranging for another person to act, as a trustee of an express trust or similar legal arrangement, or a nominee shareholder for a person other than a company whose securities are listed on a regulated market.

Under these proposals, effectively, the current rules governing financial institutions would be extended to such professionals. Such professionals would be required to undertake customer due diligence measures in the following circumstances: (1) when establishing business relationships with new customers; (2) when carrying out transactions above HK$120,000 with customers with whom they do not already have a business relationship; (3) where there are suspicions of money laundering and/or terrorist financing; and (4) when there are doubts about the veracity or adequacy of previously obtained customer identification data.3

In the first two scenarios, these professionals would be allowed to apply simplified CDD measures when dealing with specified categories of business that are considered to pose a lower risk. Simplified CDD would apply for clients who are financial institutions subject to AML regulation, listed companies, government organizations, certain types of pension schemes, investment vehicles where the managers are financial institutions supervised for AML/CFT compliance, and certain types of insurance policies.

Like financial institutions, such professionals would also be subject to enhanced CDD requirements when dealing with higher-risk situations, such as when a customer is a politically exposed person or is not physically present for identification purposes. Enhanced CDD requirements would include obtaining management approval for establishing or continuing the business relationship, and taking additional measures to mitigate the AML/CFT risk, such as enquiring with customers about their source of funds.

The proposed amendments would also codify additional recordkeeping rules, including requirements to maintain customer identification data collected, account files, business correspondence, and records of transactions with respect to each customer for a period of six years.

Enforcement of these proposed requirements would be implemented through the existing professional regulatory bodies for solicitors, accountants and estate agents. TCSPs would be required to apply for a license from the Registrar of Companies before they provide trust or company services as a business to the public; it will be a criminal offense to operate a TCSP business without a license.

**Background and Context**

These proposals are intended to enhance Hong Kong’s regulatory regime for combating money laundering and terrorist financing to bring it up to date and in line with international requirements as promulgated by the Financial Action Task Force (“FATF”), an inter-governmental body that sets standards on combating money laundering and terrorist financing.

---

3 Notably, solicitors in Hong Kong are already required to conduct such diligence by the Law Society of Hong Kong under Practice Direction P.
Hong Kong has been a member of the FATF since 1991. As most clients will be aware, Hong Kong already maintains strict requirements in respect of AML compliance and reporting that are in line with many of the world’s other financial capitals. However, in recent years, the FATF has increased its focus on CDD, including with respect to businesses that have not historically been subject to such requirements in many jurisdictions. Following the Panama Papers leak in April 2016, recent meetings of the G20 Finance Ministers have also paid particular attention to promoting greater transparency of beneficial ownership of legal persons, and the G20 has requested the FATF and the Global Forum of the OECD to improve the implementation of international standards on transparency of beneficial ownership information. The FATF and the Global Forum of the OECD are set to jointly recommend that G20 members lead by example and bring forward their plans to fully and effectively implement the FATF recommendations on beneficial ownership by the end of 2017.

The FATF has long recommended that financial institutions implement CDD measures to identify and verify customers and maintain records on customer identification and transactions for at least five years. Hong Kong has implemented such recommendations through the AMLO. However, the FATF also recommends that such requirements be applied to “designated non-financial businesses and professions,” or “DNFBPs,” which in its view present money-laundering and terrorist financing risks. Among others, DNFBPs include casinos, dealers in precious metals and stones, real estate agents, lawyers, notaries, accountants, and TSCPs. Member jurisdictions have generally been less robust about implementing CDD requirements for DNFBPs, and the FATF has in recent mutual evaluations emphasized their importance. Notably, in its recent mutual evaluation the United States was criticized by the FATF for not having CDD requirements for certain types of DNFBPs. Other jurisdictions, such as the U.K., already have such requirements, although such jurisdictions are in the minority. Hong Kong enacted the AMLO in April 2012 to implement the FATF’s recommendations relating to financial institutions. Under the AMLO, certain types of financial institutions currently have a statutory obligation to conduct CDD on their customers and keep relevant records for a specified period. However, in Hong Kong – as in certain other jurisdictions – there are currently no such statutory regulations in respect of DNFBPs. The current proposed amendments to the AMLO are expected to bring Hong Kong in line with these international recommendations.

FATF’s 2012 Recommendations (as updated in 2013, 2015 and 2016) also recommend that countries require companies to maintain information on beneficial ownership, and in 2014 the FATF published additional guidance on how to implement this. In response to this, in its latest AML Directive the EU has required that trusts and similar structures obtain and hold information on their beneficial ownership. Hong Kong’s latest proposal in requiring companies to maintain PSC registers can be seen as an effort to keep in step with these recommendations.

The proposed amendments are made in anticipation of Hong Kong’s upcoming mutual evaluation by the FATF (scheduled for 2018). In the Hong Kong Government’s view, given the recent emphasis on beneficial ownership, Hong Kong’s efforts in implementing CDD requirements will be closely examined during this upcoming evaluation.

The Hong Kong Government launched its public consultation period on the proposals on January 6, 2017. The consultation period closes on March 5, 2017. We expect the proposed amendments to become effective, potentially in modified form, at some point shortly thereafter.

For more information please feel free to contact a member of Ropes & Gray’s leading anti-corruption / international risk team.

---


5 FATF Guidance, Transparency and Beneficial Ownership, October 2014, available here.

February 20, 2017

China’s State Council Announces Major Policies to Reform the Pharmaceutical Industry

China will launch further reforms in the pharmaceutical sector as part of the healthcare reform initiatives announced by the State Council in its February 9, 2017 Circular on Several Opinions Concerning Further Reforms of the Policies Governing Drug Production, Circulation and Usage (the “Circular No.13”). The Circular No. 13 sets forth general principles of the reform. Detailed implementation measures are expected from relevant ministries, including the CFDA, National Health and Family Planning Commission (NHFPC), the Ministry of Human Resources and Social Security (MOHRSS), the Ministry of Commerce (MOC), National Development and Reform Commission (NDRC), State Administration of Industry and Commerce (SAIC), and the Ministry of Public Security (MPS).

The Circular No. 13 reinforces the government’s determination to expedite approvals for new drugs and urges generics to pass the quality consistency tests.

- Generics that are consistent with the quality of originator drugs (“high quality generics”) will be deemed interchangeable with the originator drugs. These high quality generics will be prioritized for hospital procurement. In addition, only the first three high quality generics passing the consistency test will be eligible for collective tenders for public hospitals.

- The Marketing Authorization Holder (“MAH”) system will be applicable to both new drugs and high quality generics if they are developed or manufactured in China.

- Compulsory license can be granted and enforced for any patented drugs that prevent or treat critical illness. This practice, if widely implemented, will significantly impact the competitive landscape for innovative products.

Healthcare affordability is another major theme in the Circular No. 13.

- Prices of patented and off-patent drugs must not be higher than those in the country of origin or in China’s neighboring countries. The government expects manufacturers of patented or off-patent drugs to offer price commitment when applying for marketing authorizations, and will further leverage price-volume negotiations at collective tenders to exercise its control over drug prices.

- The CFDA is responsible for establishing an ex-factory price database for pharmaceuticals to enhance surveillance and provide better intelligence for antitrust enforcement.

- Public hospitals must prioritize their use of essential drugs. The NHFPC will organize health economic studies to evaluate clinical outcomes and further rationalize the use of drugs. The performance review of public hospitals will be closely tied to the change in healthcare costs.

- Reimbursement by Basic Medical Insurance funds will be calculated based on Disease Related Groups, number of patients, or number of days in hospital. The costs for drugs and consumables will not be separately reimbursed.
• Sales of pharmaceuticals on the Internet will be promoted. Consumers can order pharmaceuticals online, with either pickup or delivery from brick-and-mortar retail pharmacies.

Last but not least, anti-bribery and anti-corruption enforcement remains high on the Chinese government’s agenda. The Circular No. 13 asks the CFDA to strengthen the administration of medical representatives. All medical representatives will have to register with the CFDA (or its local counterpart), and their registration will be timely published. More notably, medical representatives can engage only in academic promotion and technical consulting activities; they will be prohibited from selling pharmaceuticals. Failures to comply with these requirements will impact the individual credit ratings.

The Circular No. 13 will considerably impact the China strategy of multinational pharmaceutical companies. We recommend that companies carefully review and study the policies, and monitor the progress of any implementing rules associated therewith.

If you would like to discuss the foregoing or any other related matter, please contact Katherine Wang or your usual Ropes & Gray advisor.
February 23, 2017

U.S. Department of Commerce Establishes Favorable Export Control Policies for India

On January 19, 2017, the U.S. Department of Commerce’s Bureau of Industry and Security (“BIS”) published a final rule (the “Rule”) making two significant changes to U.S. export control policy with respect to India. First, the Rule establishes a more favorable licensing policy with respect to the export of most controlled items to India; second, it also expands the scope of an export license exemption program for eligible Indian entities.¹ These changes immediately follow the United States government’s designation of India as a “Major Defense Partner” on June 7, 2016, as well as other changes BIS has made in recent years to ease export controls relating to India and strengthen the U.S.-India trading relationship.² Together, these developments have established a very favorable export control policy with respect to India, which should allow both U.S. companies operating in India and Indian companies transacting with American counterparts to quickly and efficiently engage in an increased volume of trade.

New “Presumption of Approval” Standard for BIS License Applications

Under the Export Administration Regulations (“EAR”), parties seeking to export, re-export, or transfer items controlled under the Commerce Control List (“CCL”) typically first require a license from BIS. Items on the CCL, which include materials, software, and technology across a variety of sectors including electronics, telecommunications, and aerospace, among others, are classified according to a five-digit Export Control Classification Number (“ECCN”). The ECCN provides information about the nature of the product, the reason why the product is controlled, and to which countries the product may be shipped only upon receipt of a license. Previously, all license applications for exports of controlled items to India were subject to “case-by-case review” by BIS.

In contrast, the new Rule establishes a significantly more favorable “presumption of approval” standard for (1) exports and re-exports to, and transfers within, India of items subject to the EAR, including “600 Series” military items,³ for civil or military end use (including by the Government of India); (2) re-exports to countries BIS has categorized as “A:5” countries, which includes Australia and most countries in Europe; and (3) return of items to the United States, so long as the items are not intended for use in nuclear, missile, or chemical or biological weapons activities. While the change does not eliminate the need for U.S. companies operating in India or Indian companies to seek approval from BIS, the new presumption of approval standard means that companies may now routinely expect to receive regulatory approval to engage in transactions relating to almost all controlled items, including those that previously would have been subject to significantly more restrictive export control rules.

³ “600 Series” military items are items that were formerly listed on the United States Munitions List (“USML”) and subject to the International Traffic in Arms Regulations (“ITAR”) and regulated by the Department of State’s Directorate of Defense Trade Controls (“DDTC”). Pursuant to President Obama’s policy of export control reform, a number of ITAR-controlled items were shifted to the EAR, which is generally a less restrictive export regime.
Expansion of Validated End-User Program for Authorized Entities

The Rule also expanded the Validated End-User ("VEU") program applicable to certain approved Indian entities. The VEU program was established by BIS in 2007 to facilitate trade by allowing exporters to ship certain items that would otherwise be controlled under the CCL (and therefore require a BIS export license) to approved end users without a license. Currently, China and India are the only two countries eligible under the VEU program, and twelve entities have been awarded VEU status.4

Either the prospective VEU, or exporter acting on its behalf, may apply to BIS through this program, identifying both the specific destinations and the CCL items that would be covered should the application be approved. All VEU applications are then screened through a cross-departmental group chaired by the Department of Commerce and including representatives from the U.S. Departments of State, Defense, and Energy.

Prior to the Rule, controlled items could only be shipped under the VEU program if the items were for civil end use. Although the civil use limitation still applies to China,5 approved VEUs in India are now authorized to use controlled items for civil or military use, so long as the items are not transferred or used to further nuclear, missile, or chemical or biological weapons activities.6 Accordingly, while the VEU application process can be cumbersome, approval offers even greater commercial benefits for Indian end users. Any Indian company that is awarded VEU status will now be able to export items for both civil and military use without the need for a license, significantly cutting down on the regulatory burdens inherent in the BIS license application process.

Conclusion

Taken together, these changes mean that U.S. companies operating in India and Indian companies working with U.S. partners now can expect most applications to engage in transactions involving controlled items to be approved. They are also now eligible to bypass the application process entirely through the VEU program for a greater number of transactions. It has been estimated that over 810 licenses have been granted in the last five years for goods covered under the new Rule, representing $5 billion in trade.7 Accordingly, these changes are likely to have a significant impact, and should continue to expand the volume of trade and strengthen relations between the United States and India.

For more information, please contract your usual Ropes & Gray advisor.

---

4 15 C.F.R. § 748 Supp. 7 (listing the 11 Chinese entities and one Indian entity that have been awarded VEU status).
5 15 C.F.R. § 748.15(d).
6 82 Fed. Reg. at 6219.
South Korea Fines Prominent Pharmaceutical Manufacturer in Latest Anti-Corruption Enforcement Efforts

In a sign that South Korea is ramping up its anti-corruption enforcement efforts, Korean authorities announced on April 27 that they plan to levy a $48 million fine against Swiss pharmaceutical giant Novartis International AG for allegedly bribing physicians to use its products. In addition to the fine, the Korean Ministry of Health and Welfare will also suspend state insurance reimbursements for several of Novartis’ products. The fine and related penalties come eight months after Korean authorities indicted six current and former Novartis executives (along with over a dozen Korean doctors and editors of medical journals) for their role in the alleged kickback scheme, and seven months after South Korea implemented a sweeping new anti-corruption law.

Korean authorities allege that between 2011 and 2016, Novartis paid around $2.3 million in bribes to physicians, in the guise of funding of academic events, whereby Novartis would arrange for a scientific journal to host medical symposia and then would make cash “travel expense” payments to participating doctors. Novartis Korea was subject to a highly-publicized government raid last year, in which Korean prosecutors seized various documents and financial records from the company. Subsequently, Korean prosecutors criminally charged six current and former executives in August 2016, along with fifteen physicians and six medical journal publishers. Those individuals’ criminal trials are currently underway. Novartis Korea issued a statement last week that it acknowledged and accepted the government’s fine, further stating that “We do not tolerate misconduct and are continuing to invest significant efforts to fully embed a culture of compliance throughout our Korean organization.”

This is not Novartis Korea’s first domestic enforcement action. In 2011, Novartis and several other multinational pharmaceutical companies were fined by the Korea Fair Trade Commission (“KFTC”) for providing travel, entertainment and gifts to medical professionals with the objective of increasing prescriptions. Novartis Korea paid a penalty of just over $2 million to resolve the KFTC action. However, in the aftermath of the KFTC’s industry sweep, Korea introduced a “two-strike rule” intended to combat bribery in the health care sector: For a first violation, the South Korean Ministry of Health and Welfare (“MOHW”) can delist a company’s product from state reimbursement for up to one year, while a second violation can lead to permanent delisting. Per last week’s announcement, MOHW has decided to suspend various formulations of Novartis’ Alzheimer’s Disease treatment Exelon and its chemotherapy drug Zometa for three months. The Ministry will continue to reimburse the company’s other products, and it will announce its final decision on the penalty in May. In a parallel proceeding, the Korean Ministry of Food and Drug Safety had announced smaller fines and a similar three-month suspension of Exelon in March 2017. Media reports at the time suggested that the Korean government had responded to patient lobbying efforts to limit the number of suspended products, as adequate alternatives to some Novartis products did not exist in the Korean market.

Last week’s announcement appears to be the most recent indication that South Korea is bolstering its anti-corruption enforcement efforts. In September 2016, Korea implemented an expansive new anti-corruption law, the Kim Young-ran Act, that is significantly broader than the U.S. Foreign Corrupt Practices Act in several respects. For example, the new Korean statute imposes strict liability for certain payments irrespective of corrupt intent; expands the definition of covered “public officials” to include journalists and private educators; and introduces corporate criminal liability for unlawful payments made by employees and agents.
In light of these recent initiatives, pharmaceutical, medical device, and other life sciences and health care companies operating in Korea are advised to: 1) Update their policies to reflect the changes in the Korean legal landscape; 2) Provide suitable training for personnel operating in South Korea or interacting with Korean public officials worldwide on the Kim Young-ran Act and associated health care compliance requirements; and 3) Continue to ensure they have adequate internal controls regarding the appropriate provision of gifts, hospitality, and educational support to health care professionals.

For more information please contact your usual Ropes & Gray advisor.
October 19, 2016

European Health Care Compliance Challenges (And Solutions)

Life sciences and health care companies ("health care companies") rightly invest a significant amount of time and money into ensuring compliance with health care regulations in the countries in which they are based, but global companies must also consider the panoply of compliance challenges posed by the European market. This alert will address the top five health care compliance challenges facing health care companies operating in Europe, as well as simple steps that health care compliance professionals can take to address these challenges. Future alerts will address these topics in greater detail.

1. Government Interactions in Countries with Public Health Care Systems

Health care companies operating in Europe will inevitably face a higher number of government interactions than their counterparts that operate only in the United States, because nearly all of Europe has either publicly sponsored and regulated universal health care or publicly provided universal health care. Due to the public or quasi-public nature of health care in much of Europe, there are a larger number of individuals who regulators may consider government officials and with whom employees may be interacting, including doctors, nurses, and hospital administrators. Enforcement actions against health care companies are often predicated on the fact that health care professionals are government officials, and companies that interact with them regularly must be particularly aware of these risks.

Companies doing business with state-sponsored health care systems will also need to contend with sometimes complex reimbursement regimes and potential obstacles around introducing new or innovative products. Delays caused by the necessity for government approvals or reimbursement can create the incentives for bribes or facilitation payments, and the volume of government interactions increases the odds that a company may violate an anti-corruption law like the U.S. Foreign Corrupt Practices Act ("FCPA"). Health care companies must also be aware of changing local laws, such as Germany’s recent implementation of a revised Act to Combat Corruption in Healthcare which holds self-employed health care professionals ("HCPs") liable for active and passive bribery, rather than just those at state-owned hospitals who would be classified as “public officials.”¹

Solution: Companies can significantly mitigate the risks around government interactions by: 1) having clear policies and procedures around government interactions, including guidance around meals, hospitality, and sponsorship for educational events; 2) training employees who interact with government officials on these policies; and 3) monitoring compliance with these policies.

For additional information, see our Global Anti-Corruption Resources here.

2. Distribution Networks in Diverse Geographic Locations

In addition to risks from its own employees, health care companies must also be aware of the compliance risks associated with their distribution networks and foreign subsidiaries in the fragmented European market. Relying on a suite of different distributors, speaking different languages, using different currencies and with different cultures can...

¹ Sections 299 et seq. of the German Criminal Act.
create significant compliance challenges for companies across Europe. The actions of third-party distributors have been the basis for many FCPA settlements, sanction-related fines and compliance problems over the years, and companies must ensure that they have appropriate control and oversight of their third parties to limit such risks.

Solution: Companies can protect themselves by ensuring that distributors are carefully controlled, including with regards to issues around export control, sanctions, product registrations, and corruption. These steps include: 1) conducting appropriate risk-based due diligence on third-party distributors; 2) having clear written agreements that contain representations that the distributor will comply with anti-corruption, sanctions, export control and product registration regulations in the jurisdictions in which they operate, as well as limitations on the geographic area in which the distributor operates; and 3) monitoring distributor activities.

For additional information, see our White Papers and Alerts [here](#).

3. Competing Regulatory Regimes in European Countries

Another layer of complexity involved in doing business in Europe is the presence of competing regulatory regimes in the highly regulated European market. Conduct that is legal in one European country, or in the country in which a company is based, may be illegal in another European country. These regulatory regimes are subject to change at any time and keeping current with developing laws may be a challenge.

Companies should also consider ethical guidance published by professional bodies, such as the code of ethical business practices and guidelines on HCP interactions published by the medical device trade association Eucomed and the European Diagnostic Manufacturers Association (“EDMA”), the codes of practice for interactions with HCPs and patient organizations published by the European Federation of Pharmaceutical Industries and Associations (“EFPIA”), the guiding principles published by the International Federation of Pharmaceutical Manufacturers & Associations (“IFPMA”), and the Association of the British Pharmaceutical Industry (“ABPI”) code of practice in the UK, along with many other country-specific laws and sets of guidance. These trade association standards and accompanying guidance are also constantly changing. For example, on June 30, 2016, as required by EFPIA’s code on disclosures of transfers of value, EFPIA’s company members began disclosing payments to European health care providers and organizations in 33 European countries.

Solution: Companies should keep abreast of changes in regulatory regimes, including changes to transparency laws and antitrust regulations; develop a strategic approach to global and local policies that allows for flexibility to address varying and evolving legal requirements and ethical guidelines; and ensure that they seek the advice of competent local counsel in the jurisdictions in which they operate.

4. Data Privacy

Data privacy issues are a challenge for all companies, but they are a particularly tricky issue for health care companies that may be dealing with sensitive information related to patients’ health. It is even trickier in Europe, as stringent European Union (“EU”) data privacy standards will be applied and these may differ in interpretation and enforcement from country to country. Data privacy is an area of law that frequently evolves, as shown by the changes in the last year alone, including the loss of the safe harbor for U.S. companies, and the new General Data Protection Regulation that will come into effect for the EU in 2018 and have implications for all companies providing goods or services in and to European individuals, no matter where in the world the company is located.
Solution: With the focus on the new regime coming into force, any company doing business in or with Europeans should be reviewing its people, policies and procedures to ensure that they will meet the new accountability standards and remain compliant. If necessary, companies should seek advice from data privacy counsel to ensure that they comply with relevant laws in the jurisdictions in which they do business.

For additional resources, see our Alerts and White Papers [here](#).

5. New Supply Chain Disclosure Requirements under the UK Modern Slavery Act

The UK Modern Slavery Act (“MSA”) requires companies that do business in the UK with worldwide annual turnover of £36 million to annually publish a slavery and human trafficking Statement on their websites indicating the steps they have taken during the fiscal year to ensure that slavery and human trafficking are not taking place in their supply chains or in their own businesses. This broad disclosure requirement is applicable to both UK- and non-UK-based companies, including those in the health care and life sciences industries. Compliance is for fiscal years ending on or after March 31, 2016 and the Statement should be published within six months after fiscal year end. The Statement must be approved by the Board and signed by a director. Although the MSA is a disclosure-only statute that does not require companies to adopt policies and related management systems, disclosures will be used by NGOs, socially responsible investors (“SRIs”) and other stakeholders to assess ethical sourcing programs and push for change. Health care and life sciences companies often have complex multi-tier global supply chains of limited transparency. In addition, the raw materials and components in the supply chains of health care and life sciences companies (such as certain agricultural products used in pharmaceuticals and metals used in medical devices) often originate in higher risk locations that can present modern slavery risks.

Solution: If the process has not already begun, companies should start focusing on their first MSA Statements. In preparation for putting pen to paper, companies should assess human trafficking risks and current compliance procedures and determine whether enhancement is warranted. As part of this exercise, companies should benchmark compliance activities against peer companies, existing voluntary compliance frameworks and NGO and SRI expectations. Although the MSA is a simple statute on its face, Statements often take longer to prepare than companies anticipate. Many decisions will go into the approach to be taken and, especially at larger companies, many constituencies will need to weigh in on the Statement and it is likely to go through several rounds of revisions.

For additional resources, see our White Papers and Alerts [here](#) and the anti-human trafficking module of our Supply Chain Compliance and Corporate Social Responsibility Resource Center [here](#).
November 28, 2016

EU Reaches Final Agreement on Conflict Minerals Regulation – An Overview

On November 22, the EU Council, Commission and Parliament reached an informal final agreement on a conflict minerals regulation. Last week’s agreement builds upon the “political agreement” reached during June.

The regulation generally will require EU smelters and refiners and direct importers of tin, tantalum, tungsten and gold (3TG) into the EU to conduct due diligence using the OECD Guidance framework if they are sourcing from conflict-affected and high-risk areas anywhere in the world. See our earlier Alert for a more extensive discussion of the key terms of the regulation and what it means for downstream companies. Please also visit the Ropes & Gray Supply Chain Compliance and Corporate Social Responsibility Resource Center for EU source documents relating to the regulation.

The EU press conference and press releases following the final agreement were fairly light on substance, but, in addition to the above, they provide a few additional details and confirm some of the previously disclosed details of the regulation:

Importers

- Small volume importers of 3TG will be exempt, although the threshold was not included in the public announcements. The regulation is intended to cover more than 95% of all EU imports of raw 3TG. Given the high value of gold in small quantities, the EU Commission has indicated that it intends to monitor the effectiveness of the regulation as it relates to gold imports.

- The “responsible importer” concept will be retained in the final regulation. A company can become a responsible importer by declaring in writing to the competent member state authority that it follows the due diligence obligations set forth in the regulation. A list of responsible importers will be published by the Commission.

- The competent authorities in the member states will be charged with carrying out checks to ensure that EU importers comply with their due diligence obligations.

Downstream Companies

- The regulation will not require due diligence by manufacturers, importers and sellers of finished products and components. However, these companies will be encouraged to make voluntary disclosures. The EU Commission intends to develop voluntary guidance for downstream companies. It also intends to create a voluntary transparency registry where companies can report on their due diligence practices.

Conflict-Affected and High-Risk Areas

- The EU Commission will draft a handbook that includes non-binding guidelines to help companies, including small and medium-sized enterprises, with the identification of conflict-affected and high risk areas.
Next Steps in the Approval Process

- The next step is for the final agreement to be confirmed by the EU member states. The Slovak presidency of the EU Council is expected to present the agreed text to member states’ ambassadors on December 7, 2016. Early next year, the final regulation is expected to be adopted by the Council.

- Thereafter, the final regulation will move to the Parliament for a vote. The Parliament is expected to vote on the regulation during the first half of 2017.

Effective Date

- The regulation will take effect on January 1, 2021. This is a longer transition that the two year transition contemplated in earlier proposals. The transition period is intended to allow sufficient time to establish procedures and control mechanisms and prepare guidance. However, we expect that many larger downstream companies and the NGO community will push for earlier voluntary compliance.

For Further Information

If you would like to learn more about the issues in this Alert, please contact your usual Ropes & Gray attorney.

Ropes & Gray Supply Chain Compliance and CSR Mailing List

Click here to join the Ropes & Gray Supply Chain Compliance and CSR mailing list to receive Alerts, articles and program announcements relating to supply chain compliance, or to sign up for other Ropes & Gray mailing lists.

About our Supply Chain Compliance Practice

Ropes & Gray has a leading supply chain compliance and corporate social responsibility practice. We advise clients across a broad range of regulations, commodities and geographies, and our clients include leading public and private companies and trade groups from every major industry.

With on-the-ground expertise in the United States, Europe and Asia, we are able to take a holistic, global approach to supply chain compliance and CSR, to help clients efficiently and effectively structure and implement their supply chain compliance and CSR programs and mitigate risk.
The UK Modern Slavery Act – A Compliance Primer for Fund Managers

Starting this year, a significant number of fund managers based all over the world will be among the approximately 12,000 companies that will be required to publish an annual statement under the transparency provisions of the UK Modern Slavery Act. The statement is required to describe the steps that were taken during the prior fiscal year to ensure that slavery and human trafficking is not taking place in any of the subject company’s supply chains and in its own business. In this Alert, we provide an overview of the MSA and tips for compliance for fund managers. We also discuss how MSA disclosures by fund managers may be used by external constituencies.

Who Is Subject to the MSA?

The transparency provisions of the MSA have broad applicability. They apply to “commercial organisations” doing business in the United Kingdom that provide goods or services and have annual worldwide turnover of at least £36 million.

Commercial Organisations. “Commercial organisation” is defined broadly. It includes a corporation or partnership, wherever incorporated or formed, that carries on a business or part of a business in any part of the United Kingdom. A “business” includes a trade or profession.

Doing Business in the United Kingdom. The MSA does not contain a bright-line test for determining whether a commercial organisation based outside of the United Kingdom is carrying on a business or part of a business in any part of the United Kingdom. In its Guidance on the MSA, the UK Home Office has indicated that commercial organisations should apply “a common sense approach,” noting that commercial organisations that do not have a demonstrable business presence in the United Kingdom should not be required to prepare a statement.

According to the Guidance, having a UK subsidiary will not, in itself, mean that a parent company is carrying on a business in the United Kingdom, since a subsidiary may act completely independently of its parent or other group companies. However, depending upon their business activities in the United Kingdom, multiple entities in the group, even those that are not primarily engaged in carrying on a business in the United Kingdom, could be required to prepare a statement.

The Turnover Threshold. A commercial organisation doing business in the United Kingdom only will be required to prepare a slavery and human trafficking statement if, for the applicable fiscal year, it supplies goods or services and has total turnover of at least £36 million. The turnover calculation includes the turnover of the subject commercial organisation and its subsidiaries, including those subsidiaries carrying on business entirely outside of the United Kingdom.
Content of the Statement

The statement is required to indicate the steps that the commercial organisation has taken during the preceding fiscal year to ensure that slavery and human trafficking is not taking place in any of its supply chains and in any part of its own business. Alternatively, if the organisation has not taken any steps to eradicate slavery and human trafficking, it is required to indicate that.

The MSA does not require commercial organisations to adopt a human trafficking policy, conduct supply chain due diligence or put in place a compliance program. It is a disclosure-only rule, but the transparency provisions are intended to create what the UK Home Office refers to as a “race to the top,” by encouraging companies to focus on the modern slavery risks present in their business and supply chains and adopt appropriate policies and procedures to manage those risks. The transparency provisions also are intended to enable external stakeholders to evaluate company risk assessments and compliance measures and compare them against those of other companies.

The MSA and subsequent Home Office commentary indicate the following areas that a commercial organisation may wish to discuss in its statement:

- The organisation’s structure, its business model and its supply chain relationships;
- The organisation’s policies in relation to slavery and human trafficking;
- Its due diligence and auditing processes in relation to slavery and human trafficking in its business and supply chains;
- The parts of its business and supply chains where there is a risk of slavery and human trafficking taking place, and the steps it has taken to assess and manage that risk;
- Its effectiveness in ensuring that slavery and human trafficking are not taking place in its business or supply chains, measured against such key performance indicators as it considers appropriate; and
- The training regarding slavery and human trafficking available to its staff, including for supply chain management and the rest of the organisation.

However, these are recommended, rather than mandatory, disclosure topics. Commercial organisations have the flexibility to tailor their statement to their particular facts and circumstances.

The Guidance indicates that a commercial organisation that is subject to the transparency provisions must include in its statement the activities of its subsidiaries, even if a subsidiary does not independently meet all of the jurisdictional requirements of the MSA, if the activities of the subsidiary form part of the business of the parent commercial organisation.

Publication of the Statement

Dissemination. The statement must be published on the commercial organisation’s website, if it has one. If the organisation does not have a website, it must provide a copy of the statement, upon written request, within 30 days after the request is received.

The statement must be in a prominent place on the website’s home page. According to the Home Office Guidance, a “prominent place” may mean a modern slavery link that is directly visible on the home page or part of an obvious drop-down menu on that page. The Guidance indicates that the link should be clearly marked so that the contents are apparent, and it recommends a link such as “Modern Slavery Act Transparency Statement.”
**Timing.** Statements are required to be prepared annually, for the trailing fiscal year, beginning with fiscal years ending on or after March 31, 2016. Because fund managers typically have a December 31 fiscal year end, this will generally mean that the first statement required to be prepared will be for the fiscal year ended December 31, 2016.

The MSA does not contain a specific date by which a statement must be prepared and posted on the commercial organisation’s website. The Home Office Guidance indicates that organisations are expected to publish their statements as soon as reasonably practicable after the end of the applicable fiscal year, and they are encouraged to report within six months of their fiscal year end.

**Combined Statements.** The Home Office Guidance indicates that, if a parent commercial organisation and one or more subsidiaries in the same group are each required to produce a statement, the parent may produce one statement that the subsidiaries can use to meet their disclosure requirement, provided that the statement fully covers the steps that each of the commercial organisations required to produce a statement has taken in the relevant fiscal year.

**Approval and Signature Requirement**

The statement must be approved by the board of directors (or equivalent management body) and signed by a director or the equivalent if the commercial organisation is a body corporate. If the entity is a limited liability partnership, the statement must be approved by the members and signed by a designated member. If the commercial organisation is a limited partnership registered under the U.K. Limited Partnerships Act, it must be signed by a general partner. If the organisation is any other kind of partnership, the statement must be signed by a partner.

**Getting Started – Observations and Selected Compliance Recommendations**

**Start by Assessing Applicability.** As an initial matter, fund managers should assess whether any of their management companies or other group entities must prepare a statement and, if so, which entities. A significant number of managers have offices in the United Kingdom and will meet the “doing business” requirement of the MSA transparency provisions. In most cases, the statement only will be required to cover a portion of the business activities and operations of managers based outside of the United Kingdom due to the manner in which their global operations are structured. Up-the-chain and sister entities are not required to be included in an MSA statement unless they independently meet the requirements of the MSA. However, some managers will elect to discuss their risk assessment and compliance activities for their entire consolidated group.

**Review Existing Policies and Procedures and Consider Whether to Make Enhancements.** As noted earlier in this Alert, the transparency provisions of the MSA only require disclosure. They do not require a modern slavery or social compliance policy or particular compliance procedures to be put in place. However, in connection with preparing an MSA statement, among other things, managers should review applicable portions of existing management company and investment policies and pre-and post-investment procedures that address human and labor rights such as modern slavery. These should be reviewed against any publicly disclosed policies and procedures of other managers with comparable strategies, as well as against any limited partner expectations, guidelines and commitments. Managers also should assess the extent to which existing human and labor rights policies and procedures align with NGO guidance and whether they are sufficient to mitigate reputational and other potential risks relating to modern slavery.

Managers that have not yet assessed modern slavery risk or extended environmental, social and governance (ESG) programs to cover modern slavery – which includes most managers – should take a gradual approach. A significant portion of first time MSA statements by managers (and commercial organisations generally) will indicate that their modern slavery risk assessment and the establishment of appropriate compliance procedures remain works in process. External constituencies recognize that it takes time to develop and implement a tailored compliance approach. The Home Office Guidance echoes this view and notes that first statements may indicate how the commercial organisation is starting to act on the issue of modern slavery and its planned actions to investigate or collaborate with other stakeholders to effect change.
Write Your MSA Statement for Limited Partners and NGOs. Strictly from a compliance standpoint, a manager could take a narrow approach in drafting its MSA statement, hewing to the literal requirements of the Act. Unlike manufacturers and sellers of products, fund managers do not have supply chains. In addition, entities in which they invest are typically not considered part of the manager’s own business.

However, the consideration of ESG factors at the management company level and in investment decisions and ongoing portfolio management is an increasing area of focus for limited partners, especially European pension fund investors investing in private equity funds and other funds with illiquid strategies. Limited partners are likely to start using MSA statements as part of their ESG assessment. In addition, NGOs already have begun reviewing and ranking MSA statements, and more rankings, including by industry, are expected later in the year. Larger fund managers are the most likely to be included in industry rankings and, to the extent their statements and related compliance efforts are viewed as deficient, targeted for NGO engagement.

For all of these reasons, managers generally will be better served by a more robust MSA statement. For example, managers should consider discussing, to the extent applicable, (1) their principal investment strategies, (2) how human and labor rights, including modern slavery, are addressed in their ESG policies, (3) how modern slavery risk is assessed and (4) any related pre- and post-investment compliance procedures and engagement with companies in which the manager invests. The manager also should consider indicating whether it is a signatory to or otherwise following particular responsible investment or human rights guidelines, such as the UN-supported Principles for Responsible Investment, the Private Equity Growth Capital Council Guidelines for Responsible Investment, the UN Global Compact, the UN Guiding Principles on Business and Human Rights, the IFC Performance Standards on Environmental and Social Sustainability and/or the Equator Principles. It also should consider discussing whether it encourages companies in which it invests to follow particular human and labor rights guidelines and codes of conduct relevant to their industries.

External stakeholder expectations will be greatest for managers of private equity, infrastructure and real estate funds, as well as other managers that make significant illiquid investments, such as some credit fund managers. To the extent that it is not practical for the manager to consider social factors in its investment decisions for some or all of the asset classes in which it invests, the manager should consider discussing that in its statement as well.

Align the Statement with Other ESG Disclosures, Statements and Commitments. At many companies, ESG communications lack consistency. Fund managers are no different in this regard. Managers should ensure that their MSA statements are consistent with ESG guidelines in investment policies, any ESG statements and commitments made to limited partners and other publicly facing ESG statements and disclosures. In addition, for private equity firms and other managers that make control investments, MSA and California Transparency in Supply Chains Act statements published by portfolio companies should be consistent with any ESG guidelines of the manager that are applicable at the portfolio company level.

Approach MSA Compliance as a Process, Not a Project. An MSA statement must be prepared annually. As a recurring requirement, a member of the legal, compliance or operations group should be assigned ongoing responsibility for the statement. Disclosures will evolve as commercial organisations, including fund managers, continue to assess modern slavery risk and implement and enhance their modern slavery compliance procedures. Furthermore, as has been the case with other mandatory and voluntary ESG disclosures, other year-over-year enhancements to disclosures will be made as limited partners, NGOs and other external constituencies publish expectations documents, advocate for specific practices and rank compliance efforts.

About Our Supply Chain Compliance and CSR Practice

Ropes & Gray has a leading supply chain compliance and corporate social responsibility practice. We advise clients across a broad range of regulations, commodities and geographies, and our clients include leading public and private companies, including fund managers, and trade groups from every major industry.
With on-the-ground expertise in the United States, Europe and Asia, we are able to take a holistic, global approach to supply chain compliance and CSR, to help clients efficiently and effectively structure and implement their supply chain compliance and CSR programs and mitigate risk.

For further information on our supply chain compliance and CSR practice or if you would like to learn more about the topics in this Alert, please contact your usual Ropes & Gray attorney or contact us here.

**Ropes & Gray Supply Chain Compliance and CSR Mailing List**

Click here to join the Ropes & Gray Supply Chain Compliance and CSR mailing list to receive Alerts, articles and program announcements relating to supply chain compliance and corporate social responsibility, or to sign up for other Ropes & Gray mailing lists.

**Ropes & Gray Supply Chain Compliance and Corporate Social Responsibility Resource Center**

As part of our commitment to excellence in this area, we have developed the Resource Center as a free educational tool for our clients, friends and other stakeholders. The Resource Center is the most extensive complimentary collection of supply chain compliance resources and is frequently updated to reflect new developments in this dynamic area. Click here to go to the Resource Center.
August 17, 2016

**Mexico Enacts a Sweeping New Anti-Corruption Regime, Accompanied by a Public Apology from President Peña Nieto and Increased Attention on Mexico’s Energy Sector by U.S. Regulators**

After an aggressive grassroots campaign, Mexican President Enrique Peña Nieto recently announced the enactment of sweeping changes to Mexico’s anti-corruption regime. The new law is a significant step toward transparency in a country that consistently ranks among the most corrupt in the region and the world. Almost as noteworthy, President Peña Nieto publicly apologized for his own involvement in a conflict-of-interest scandal that has plagued his administration for years.

**The New Legislation in Mexico**

The new legislation was originally proposed in early 2016 to the Mexican legislature through a unique citizen petition process primarily aimed at increasing transparency of public sector officials. More commonly known as the “three of three” proposal, this original legislation would have required three separate stakeholder groups—public officials, close relatives of public officials, and any individual or entity that is the beneficiary of a government contract—to publicly disclose three pieces of personal information: (1) an accounting of their personal assets, (2) certain tax information, and (3) an accounting of their economic and beneficial interests. Ultimately, the Mexican government stopped short of adopting the “three of three” proposal in full. Specifically, the new law does not require recipients of government contracts to disclose personal assets, tax information or economic interests. It also allows public officials to withhold information “whose publication may affect privacy or personal data protected by the Constitution.”

While some of the transparency provisions of the legislation were pared back, the new law goes beyond transparency to enhance the Mexican anti-corruption regime more broadly. For the first time, the new law creates an independent anti-corruption prosecutor. It also creates whistleblower protections for individuals and implements methods to enhance cooperation across federal, state, and municipal enforcement authorities as well as with the U.S. government and other international regulators.

The regulations, which will come into effect on July 19, 2017, also provide for significant criminal and administrative sanctions for private parties and legal entities that are found to have engaged in bribery, collusion in public bid procedures, influence peddling, wrongful use of public resources, or wrongful recruitment of ex public servants, among other acts. Individuals face sanctions of up to twice the amount of the acquired benefits (or if no tangible benefit, around $600,000 USD), temporary ineligibility to participate in procurement, leases, services or state-owned projects for a period ranging from three months to eight years, and compensatory and/or punitive damages. Legal entities face similar sanctions—up to twice the amount of the benefit (and up to $6 million USD if no monetary benefit)—and could be deemed ineligible to participate in procurement, leases, services or state-owned projects for up to 10 years. Entities could also be subject to suspension of activities for a period ranging from three months to three years, partnership dissolution, and compensatory and/or punitive damages. Along with the new penalties, the new regulations provide for some partial defenses for entities and persons charged with violating the...
law. For example, legal authorities will give credit for the existence of a current compliance or integrity program that includes effective reporting and whistleblower protection tools. Entities may also receive credit for self-reporting misconduct and collaborating with government investigations, and a person who has committed a serious administrative offense can confess and fully and continuously cooperate with authorities in exchange for a reduction of 50-70% of the total amount of his or her sanction.

**President Peña Nieto’s Public Apology**

In an unprecedented step, Peña Nieto issued a public apology, during the press conference announcing the legal reforms, for the distraction of an ongoing conflict-of-interest scandal that has plagued his administration for nearly two years. Beginning in November 2014, Mexican media outlets started reporting that a major government contractor had sold a luxurious, seven-bedroom home valued at $7 million to Peña Nieto’s wife, first lady Angélica Rivera. The contractor who designed and sold the home to Rivera, Grupo Higa, had been part of a consortium of companies who won a multibillion-dollar infrastructure contract during Peña Nieto’s presidency. What is more, one of the contractor’s chief executives was a close friend of Peña Nieto. Rivera and Peña Nieto maintained that the purchase of the home was legitimate, and a government-sponsored investigation found no evidence of wrongdoing on the part of either member of the first family. However, during his press conference, Peña Nieto apologized for the effect the controversy had on public perception of his administration, though he maintains that he had not broken any laws and that combatting corruption would continue to be a principal goal of his administration.

As evidenced by the promulgated legislation and Peña Nieto’s own words during the signing of these regulations, corruption is a key area of focus both for the Peña Nieto administration and the government watchdogs that were responsible for the grassroots effort to mobilize the Mexican legislature.

**Continued U.S. Enforcement of Conduct in Mexico: Key Energy Settlement**

The changes to Mexico’s anti-corruption enforcement regime occur at the same time that regulators in the U.S. have again demonstrated that corruption in Mexico remains an enforcement priority. On August 11, 2016, the U.S. Securities and Exchange Commission announced that Key Energy Services, Inc., a Houston-based energy company, would pay $5 million USD in disgorgement for violations of the internal controls and books-and-records provisions of the Foreign Corrupt Practices Act. The Commission explained that its investigation yielded evidence that Key Energy’s Mexican subsidiary had made payments to an employee at Pemex, Mexico’s state-owned oil company, in order to induce the employee to provide information that would benefit Key Energy while negotiating contracts with Pemex. Key Energy paid the Pemex employee through a third-party consulting firm and recorded the payments as legitimate business expenses in the records of the Mexican subsidiary.

The Key Energy settlement and recent changes in Mexican law prove that the “state of play” regarding interactions with government officials in Mexico is shifting, becoming increasingly fraught with risk. Given this reality, companies should consider how their past or future conduct may make its way into the public sphere and monitor the practical application of these new laws on the day-to-day operations of their businesses. For example, companies doing business in Mexico can protect themselves by ensuring they perform comprehensive, risk-based due diligence on engaged and prospective third parties, training and educating their employees on the risks associated with doing business in Mexico, and examining the company’s internal controls to ensure that the company has properly accounted for its funds, its presence in the country, and any interactions with government officials.

For more information please feel free to contact a member of Ropes & Gray’s leading anti-corruption and international risk team.
September 28, 2016

Top 10 Anti-Corruption Red Flags In Latin America

Latin American countries continue to be a source of potentially lucrative investment opportunities for U.S. and multinational corporations. At the same time, operating in Latin America may present corruption-related challenges under the U.S. Foreign Corrupt Practices Act. Identifying corruption under the FCPA, however, is often not as easy as catching culprits in a red-handed exchange involving envelopes teeming with cash. Rather, symptoms of these issues are often identified through commonly observed violations of the FCPA’s books-and-records and internal-controls provisions.

This article highlights 10 red flags related to the FCPA’s accounting provisions, as well as enforcement actions undertaken by the U.S. Securities and Exchange Commission and U.S. Department of Justice for conduct occurring in the region. Although these red flags are not exhaustive, they may help serve as a guide to evaluating risk under the FCPA while operating in high-risk Latin American markets.

Books-and-Records Red Flags

First, we have identified five common warning signs related to the FCPA’s books-and-records provision. The books-and-records provision requires companies to “make and keep books, records, and accounts” that “accurately and fairly” reflect its transactions and to “devise and maintain a system of internal accounting controls.”

1. Inadequate Supporting Documentation

Problematic recordkeeping is a common red flag for potential FCPA accounting violations. One key to maintaining proper books and records is ensuring that transactions are supported by complete documentation.

There is a wide spectrum of issues that may be encountered with supporting documentation for transactions. Sometimes, it is as simple as incomplete forms. In other instances, companies may make large payments that are supposedly “consulting fees” without attaching documents that show work was done. This potential violation may also involve vendor documents, such as invoices or bills of lading, where the address used was fake, a residential home, or simply vacant.

---

1 While the primary focus of this article is on investigations or enforcement actions by the U.S. Securities and Exchange Commission (“SEC”) or the U.S. Department of Justice (“DOJ”), governments in Latin America seem to have also ramped up their own anti-corruption laws and efforts. Many, if not all, of the areas addressed by this article are being identified as anti-corruption issues in local Latin American investigations and enforcement actions. In addition, these considerations are not just important in terms of evaluating FCPA risk; issues in any of these areas may also be indicative of exposure to fraud or other types of accounting misconduct.

2 Specifically, in addition to prohibiting the payment of bribes, the FCPA requires companies to (1) “make and keep books, records, and accounts” that “accurately and fairly” reflect its transactions and (2) “devise and maintain a system of internal accounting controls.” 15 U.S.C. § 78dd-1, et seq. Another prominent anti-corruption statute, the UK Bribery Act, does not have explicit provisions on books and records and internal controls, but does offer an “adequate [compliance] procedures” defense to liability. See UK Bribery Act 2010 c. 23, § 7.

These types of violations appear to be on the government’s radar, as shown by recent enforcement actions involving instances where improper payments were disguised as legitimate transactions using inadequate or falsified supporting documentation. Last August, Vicente E. Garcia, a former software executive, pleaded guilty to conspiracy to violate the FCPA for allegedly using “sham contracts” and “false invoices” to disguise bribes to Panamanian officials.4

2. Misreporting Payments

A second way for noncompliant employees to pass off improper payments as legitimate is by mischaracterizing or misreporting transactions. Transactions recorded in cost accounts which are not product-related (e.g., commissions, employee advances, travel and entertainment, marketing or “other”) may be analyzed to identify such transgressions. Improper payments may be misclassified under such accounts.

This warning signal seems to appear often in Latin America-focused actions by government agencies. For example, former top executives at brokerage firm Direct Access Partners, who were charged by the SEC and DOJ in April 2014, had disguised reimbursements for bribes paid to an executive at a state-owned Venezuelan bank out of their and other employees’ personal funds.5

Executives at aerospace corporation Embraer SA similarly concealed bribes to a Dominican official by booking them as consulting fees in a separate transaction that never happened. These executives now face criminal charges by the Brazilian government, at the same time that Embraer is subject to an ongoing investigation in the United States.6

Another example of this issue can be found in a March 2016 settlement between the SEC and Novartis AG for $25 million.7 Novartis’ subsidiary allegedly made improper payments to induce foreign officials to prescribe or recommend Novartis products, which were then falsely recorded as legitimate selling and marketing costs in its books.

3. Transactions Lacking a Business Purpose

Another method for making potentially improper payments is the provision of benefits to nonemployees without a legitimate business purpose. This may include holiday gifts, extravagant entertainment, travel expenses for family members, or even extended visits or tours added on to “business trips.” In order to win government contracts, Dallas Airmotive Inc., an aircraft engine service provider, allegedly provided Latin American officials with vacations and other benefits and faced a $14 million criminal penalty.8

In fact, one need look no further than Operation Car Wash, the largest corruption scandal in Brazil’s history — and perhaps the largest bribery scandal in modern times.9 Officials at Brazil’s state-owned oil company, Petrobras, allegedly received inappropriate or extravagant gifts and inappropriate benefits of all kinds, from Rolex watches to $3,000 bottles of wine, and from yachts to prostitutes.10

4. Off-the-Books Records or Transactions

Companies should also be on the lookout for activity which is “off the books,” a possible indicator that something improper may be hidden. Common examples of this in Latin America are debt that is not recorded on a balance sheet, reconciliations reflecting inflated sales, and fictitious inventory. These “off-the-books” transactions can be used to hide proprieties or obscure the actual financial performance of a company.

An example of this misconduct is the December 2010 charge against French telecommunications company Alcatel-Lucent SA for paying bribes to win business in Honduras, Costa Rica and elsewhere. To hide these payments, Alcatel’s subsidiaries allegedly either improperly recorded them as consultant fees or simply left them “undocumented.” Alcatel paid more than $137 million in the settlement.

5. Pricing Discrepancies

Large differences in pricing — especially when prices do not match a written agreement — are another sign of potentially improper transactions. Excess funds resulting from large discounts, premium charges, or commissions might be used for bribes.

For example, as Kara Brockmeyer, chief of the SEC Enforcement Division’s FCPA Unit, explained, Garcia, the software executive, “falsified internal approval forms and disguised his bribes as discounts.” Similarly, in April 2016, the SEC entered into settlements with seven individuals for their alleged roles in the kickback scheme involving Direct Access Partners described above; the funds for the improper payments were procured in part through large markups and markdowns. As the FCPA guide notes, companies should be wary of large commissions provided to sales agents or discounts to distributors.

Red Flags for Internal-Controls Violations

Beyond simply prohibiting bribes and requiring proper books and records, the FCPA requires that companies devise and maintain a system of internal controls. Below are five potential indications of violations of the FCPA’s internal-controls provision.

6. Override of Internal Controls

Regulators continually emphasize that an effective compliance program is only as strong as the response of and adherence by company management. As Stephen L. Cohen, associate enforcement director of the SEC, urged in October 2013, “A strong compliance and ethics program must start with proper governance, including a tone at the top built on actions rather than words.” Internal controls which are ignored by management are meaningless in the eyes of government regulators.

To that end, it is a troubling red flag when management or others override or intentionally circumvent established internal controls. For instance, management might approve manual expense reports without sufficient documentation or change prices for customers outside of a company’s enterprise system. Further, payments may be made outside of
the general ledger system or multiple payments may be made to the same third party which are just below established mandatory review amounts.

It appears that regulators are focused on this red flag, as shown by recent actions and investigations. For example, Embraer’s executives allegedly recorded bribes paid to a middleman as consulting fees in an effort to get around its compliance department, which had originally prevented the full transfer of the bribes.17

7. Inadequate Screening of Third Parties

One key to developing an effective compliance program is implementing controls to ensure proper oversight over third parties, including a third-party due diligence program. Without a program to screen third parties for legitimacy, a company may be paying vendors or agents that pay bribes, circumvent import and export laws, or even do not exist.

A due diligence program should identify whether a prospective third-party business partner does business with or is a government official, in order for a company to understand the level of FCPA risk. The FCPA covers payments to a much broader group than what is customarily considered government officials. For instance, employees of public medical facilities — which are common in Latin America — are considered by SEC and DOJ to be foreign officials.18 Reviewing and categorizing payment recipients to identify employees of state-owned medical facilities in Latin America are important ways for a company to oversee its third-party business partners.

An inadequate due diligence program can have substantial FCPA risks. According to Brockmeyer, a company cannot “possess[] a ‘check the box’ mentality when it [comes] to third-party due diligence” or “simply rely on paper-thin assurances by employees, distributors, or customers.”19

8. Failure to Internally Assess Compliance Programs

A core aspect of developing a comprehensive system of effective anti-corruption internal controls and policies is a risk assessment to determine whether the controls are adequate.20 Many of the FCPA issues identified in this article occurred not because companies lacked good policies on paper but, rather, because the companies’ employees or third-party partners did not have an awareness of, and an emphasis and structure to ensure, FCPA compliance.

An internal-control failure could subject a company to substantial financial consequences. Tyson Foods Inc. entered into a multimillion-dollar settlement in 2011 for, according to the SEC, its “lax system of internal controls that failed to detect or prevent” illegal payments to government-employed inspection veterinarians in Mexico.21 Financial consequences may involve not only direct penalties, but also requirements to implement extensive new compliance initiatives and years of engaging a third party to act as a compliance monitor.

9. An Inadequate Internal Audit Program

A rigorous self-monitoring program, including a robust internal audit function, is a crucial part of a system of effective internal accounting controls. A company’s internal audit team should test transactions and supporting documentation, and follow up on negative findings. In order to be equipped to address anti-corruption risks, a company’s internal audit team should be trained on the FCPA and other applicable anti-corruption laws.

The importance of self-monitoring is underscored by statements from the SEC. Brockmeyer has emphasized the importance of implementing internal controls to stop patterns of illegal payments to win business in Latin America and elsewhere, including detecting improper payments and gifts. It is important for companies to maintain an adequate internal audit function to detect and remediate corruption-related risks and issues.

10. Use of Shell Companies

Companies subject to the FCPA should also be wary of the use of shell companies by their Latin American subsidiaries. Shell companies can be another tool to facilitate “off-the-books” transactions, a red flag described above, which can include payments to foreign officials.

The recently released “Panama Papers” have turned a spotlight on this issue by providing examples of individuals, governments, and corporations (including ones in Latin America) using shell companies to hide assets from tax and regulatory authorities. While analysis of these documents is ongoing, to date more than 10 million released records from the Panamanian law firm Mossack Fonseca name over 200,000 anonymous offshore companies around the globe. Given the reality of conducting business in Latin America, it may be prudent for a corporation subject to the FCPA to require information on the beneficial owners of third parties to whom payments are made, depending on the type of company and its interactions with other third parties.

It is clear that the U.S. government takes these risks seriously. One of the Direct Access executives who pleaded guilty allegedly paid kickbacks to a shell entity controlled by the Venezuelan official. Likewise, Terra Telecommunications Corp. paid almost $1 million to shell companies to be used for improper payments to officials at Haiti’s state-owned telecommunications company, leading to convictions of Terra’s former executives.

Conclusion

The FCPA mandates that companies maintain accurate books and records and a robust system of internal accounting controls. While not as attention-grabbing as the anti-bribery provision, a company’s failure to deal with these 10 red flags could be a signal of — or result in — FCPA violations in Latin America and beyond. Even in the absence of charges related to the anti-bribery provision, the U.S. government continues to investigate and prosecute companies and individuals for violations of the accounting provisions of the FCPA as a result of their operations in Latin America.

Given the region’s history and current risk profile, companies seeking to take advantage of business opportunities in Latin America should ensure they develop accounting processes and controls designed to reduce corruption-related risk and to identify and prevent red flags under the FCPA.

Rajal Dubal is a director in AlixPartners’ financial advisory services practice in New York. Adam Tymowski is a director in AlixPartners’ financial advisory services practice in Chicago. Nicholas Berg is a partner and David Rojas is an associate in Ropes & Gray’s Chicago office.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

---

Republished with permission from Law360.
December 20, 2016

Update on the Anti-Corruption Landscape in Mexico

After an aggressive grassroots campaign, in mid-2016, the Mexican government signaled substantial progress in its fight against corruption when it adopted a new anti-corruption program. The new legislation promised increased transparency and accountability of public officials and energized the international community about Mexico’s commitment to fight its long-standing corruption problems. Since enactment, however, progress towards implementing the provisions of the new law has slowed, leaving many questions about its future unanswered.

Anti-Corruption Regime in Mexico

Mexico’s anti-corruption enforcement regime (the “National Anti-Corruption System”) was approved by President Peña Nieto on July 18, 2016. The National Anti-Corruption System, which will come into effect on July 19, 2017, provides for severe sanctions against individuals and entities that are found to have engaged in bribery, collusion, and influence peddling, among other acts. For instance, individuals face sanctions of up to twice the amount of the acquired benefits, temporary ineligibility to participate in procurement, leases, services or state-owned projects, and compensatory and/or punitive damages. Legal entities face similar sanctions—up to twice the amount of the benefit—and could be deemed ineligible to participate in the aforementioned projects for up to 10 years. Entities could also be subject to suspension of activities, partnership dissolution, and compensatory and/or punitive damages. The National Anti-Corruption System offers partial defenses, such as the existence of a current compliance or integrity program that includes effective reporting and whistleblower protection tools. Entities may also receive credit for self-reporting misconduct and collaborating with government investigations.

Along with the promulgation of stringent sanctions, the National Anti-Corruption System also created the role of independent anti-corruption prosecutor—the first of its type in Mexico’s history—to operate independently of the Mexican government. Importantly, National Anti-Corruption System is designed to enhance cooperation across federal, state, and municipal enforcement authorities and foreign authorities including the U.S. government.

Although the enforcement regime provides much needed transparency for a country riddled with corruption, we have yet to see the National Anti-Corruption System in action. Since its adoption nearly five months ago, there has been very little progress in establishing the framework needed to effectively implement the key provisions. In fact, the Mexican government has yet to even appoint the anti-corruption prosecutor. Recent developments could further exacerbate the period of stagnation.

Obstacles to Enforcement

In September 2016, President Peña Nieto’s approval rating fell to an all-time low of 22% amidst reports that citizens were unhappy with his failure to fight crime, drug trafficking, corruption, and poverty. President Peña Nieto was harshly criticized for his decision to meet with Donald Trump in the summer of 2016 due to the threats Trump made towards Mexico throughout his campaign. Without the backing of his countrymen, President Peña Nieto may lack the necessary support in the legislature to roll out an effective National Anti-Corruption System next July.

Donald Trump’s election could further complicate the potential effectiveness of the National Anti-Corruption System. As President-elect Trump’s inauguration nears, the media continues to speculate about his immediate impact. For example, Mexico’s economic outlook may turn squarely on the resolution of the North American Free Trade Agreement (“NAFTA”). Trump has publicly stated his intent to “tear up” or drastically alter the current version of NAFTA, which was signed in 1994 and permits free trade between Canada, Mexico, and the U.S.
the fact that 80% of Mexican exports are purchased by the U.S., any change to NAFTA will impact Mexico’s economy. Despite his many public statements about NAFTA, many believe that Trump is using the NAFTA threats to pressure Mexico into accepting tariffs on certain products to spur relocation within American borders of manufacturing facilities owned by American companies.

Practically speaking, a cooling-off period is likely to occur before any drastic measures are taken. The U.S. and Mexico share common interests in improving cross-border relations and promoting economic growth, which will require ingenuity and compromise. One step in the right direction is Mexico’s enactment of the National Anti-Corruption System. The U.S. economy will certainly share in the benefits of a less corrupt infrastructure in Mexico. Nevertheless, it will require a significant amount of resources to enforce the stringent measures detailed above. Amidst the never-ending flow of speculation, the outlook for an effective anti-corruption regime in Mexico is uncertain.
March 30, 2017

A Judicial Reinterpretation of the Brazilian Constitution’s Right to Health Care

In recent years, there has been a spike in right-to-health litigation in Brazil wherein citizens seek court orders mandating that certain medications be dispensed through the public health system (Sistema Único de Saúde—“SUS”). Now a ubiquitous term, the “judicialization of health care” (“judicialização da saúde”) is often considered to be a last resort for citizens when the state fails to meet their needs. The critical issue is that patients have been using free legal assistance and a responsive judiciary to procure costly drugs and treatments that are not included on the list of pre-approved drugs and treatments covered by the SUS. Consequently, the SUS is required to fund high-cost drugs that meet the needs of a small group of people, but are not necessarily of broader use to the collective citizenry. Furthermore, many court-backed judicial determinations that mandate the provision of certain drugs may contradict administrative policies and challenge cost-cutting governmental efforts.

Given the increasingly dire state of the Brazilian economy, there are concerns over the budgetary burden imposed on the SUS by judicial procurement. In the near future, Brazil’s Federal Supreme Court (Supremo Tribunal Federal—“STF”) will be voting on whether the SUS should cover high-cost drugs not included on government formularies. If the judiciary reinterprets the constitutional right to health care and limits its scope, there could be broad implications for the demand of non-formulary drugs.

The Judicialization of Health Care

The 1988 Brazilian Constitution declared health a “right of all persons and the duty of the State,” which prompted the creation of the SUS, extending health coverage to all citizens. The Constitution underscored the autonomy of the judiciary from the government, which established the public defender’s offices to give the indigent access to the justice system. The right to medication as part of the constitutional right to health stems from the passage of a landmark law in 1996 establishing free universal access to antiretroviral therapies for HIV-infected individuals, as well as from Ministry of Health policies and a 2000 ruling by the STF.

The federal, state and municipal governments are responsible for purchasing and distributing SUS medicines according to specific drug formularies. In general, the formularies comprise generic drugs bought in bulk in a tax-exempt, competitive bidding process. The federal government is responsible for financing higher cost and more complex treatments (i.e., “exceptional medicines”), while the states oversee the distribution of these federally subsidized treatments. The state governments provide intermediate-cost and medium-complexity treatments (i.e., “special medicines”) that do not appear on the federal or municipal formularies. The municipal governments cover low-cost “basic” drugs that are dispensed at local public pharmacies.

There are three broad categories of requests from Brazilian citizens who rely on judicial procurement to obtain medication. The first category encompasses patients who seek an out-of-stock product that is already on the SUS formularies list. The second category includes patients who seek products that have yet to be approved by the National Health Surveillance Agency (Agencia Nacional da Vigilancia Sanitaria—“Anvisa”), which is responsible for the regulation and approval of pharmaceutical drugs. Because federal law prohibits the supply of medicine that is not authorized by Anvisa, neither the SUS nor health insurance companies will readily supply a drug that has yet to be registered with the agency. However, if a judge determines that no other therapeutic alternative is available for a plaintiff, the court may grant an injunction to access medicine not yet cleared by Anvisa. The third category comprises
patients who search for drugs that have been approved for sale in Brazil by Anvisa, but are not yet included on the SUS list. The high costs resulting from the judicialization of health care are generally attributed to this last group.

When a citizen is granted an injunction, the government deposits money in the plaintiff’s account to pay for the medication. These transfers are commonly referred to as “deposits to judicial accounts.” The purchase of a court-granted medication occurs two to five days after the injunction is granted, and generally involves brand-name drugs not included on SUS pharmaceutical distribution lists. This short time frame thus forces the state to buy from the market on a case-by-case basis, which eliminates price competition and results in inflated drug prices. The occurrence of “deposits to judicial accounts” increased 227% from 2012 to 2015, leading to the distribution of $440 million reais (approximately USD $143 million).

**Intermediary Role of the Judiciary**

There is consensus among public administrators that the judiciary is overstepping its role by promoting the judicialization of health care. The district and appellate judges who preside over the lawsuits in question have given broad deference to physicians’ prescriptions and individual circumstances, which undermines state efforts to rationalize pharmaceutical use and curb high spending. Furthermore, the judges’ limited technical expertise and lack of understanding of the SUS’s drugs selection process pose significant administrative and economic challenges.

The judicial procurement of medicine frequently overlooks and contradicts established public health policies. For example, generic drugs were approved in Brazil in 1999 under Law n. 9.787/1999, which instructed that the government give preference to generic drugs. However, in reality, court-backed judicial determinations often grant injunctions for brand-name drugs, which are not likely to be available yet in generic form. By distributing drugs that have not yet been approved by Anvisa, courts also challenge the agency’s role in regulating efficacious and safe pharmaceutical drugs. Courts often fail to enforce the Ministry of Health’s guidelines for treatment criteria that mandate independent expert opinions and reviews of new medical evidence. Critics recommend that if this practice continues, the courts should demand expert assessment of the safety and efficacy of off-list medications or drugs not registered for sale in the country before ruling for or against their provision for individual plaintiffs.

In September 2016, the eleven judges of the STF—the “ministers”—were slated to vote on whether the government should pay for high-cost drugs and treatments not included on government formularies. Ultimately, only three ministers voted in September, as one minister, Teori Zavascki, requested to delay the vote. Zavascki later died in an airplane accident in January 2017, and the vote was never rescheduled among the remaining ministers. On February 22, 2017, the Senate approved interim President Michel Temer’s nomination to replace Zavascki, Alexandre de Moraes. Although a rescheduling of the vote on the judicialization of health care has not yet been announced, many observers predict that it will occur within the year.

**Paradigm Shift Implications**

A vote by the STF to prohibit the SUS from paying for high-cost drugs and treatments excluded from government formularies could result in more limited access to specialty pharmaceuticals for Brazilian citizens. However, the practice of seeking medication through judicial procurement likely will not cease, as citizens will continue to file lawsuits to obtain out-of-stock drugs that are already registered with the SUS. Thus, as part of any consideration of whether to pay for specialty pharmaceuticals, the SUS should consider the need to regularly incorporate new medicines into its public distribution lists. If the SUS decides to include new medicines more frequently, pharmaceutical marketing efforts may shift to formulary access discussions. For their part, pharmaceutical manufacturers should closely monitor the judicial procurement system in Brazil and be mindful of the dynamics involved in formulary placement in this complicated market.