McDermott Will & Emery

International News

ISSUE 3 2014

Focus On **Compliance**

How One Compliance Programme Can Meet Global Challenges p.4 >>
E-Discovery: Pre-Emptive Measures to Keep Costs Down p.14 >>

Editor

Hugh Nineham
+44 20 7570 1425
hnineham@mwe.com

Managing Editor

Rohan Massey
+44 20 7577 6929
rmassey@mwe.com

Publication Editors

Kate Hinze

Ellen McDonald

Contributing Authors

Terry Ahearn, Ping An, William Brown, Glenn Engelmann, Wolfgang Freiherr Raitz von Frentz, Todd Harrison, Carla Hine, Karin Holloch, Bettina Holzberger, Clemens Just, Obiamaka Madubuko, Rohan Massey, Heather Egan Sussman, Kian Tauser, Volker Teigelkötter, Emmanuelle Trombe and Neal White.

To learn more about *International News* or our international practice, visit www.mwe.com/international/. To be added to our mailing list or report a change of address, please e-mail mcdermottnews@mwe.com. To sign up to receive substantive communications from McDermott, visit www.mwe.com/subscribe/.

McDermott Will & Emery

International News

CONTENTS

In This Issue

Hugh Nineham 3

Focus on Compliance

How One Compliance Programme Can Meet Global Challenges

Karin Holloch and Neal White 4

Avoiding Common Pitfalls During Internal Investigations

Obiamaka Madubuko and Wolfgang Freiherr Raitz von Frentz 6

Defending Against Charges of Corruption in China: The Best of Chinese and US Styles

Ping An 8

EU and US Data Protection Standards – Finding Common Ground

Rohan Massey and Heather Egan Sussman 10

Disclosure Requirements in the Health Care Sector: The Sunshine Act and Its European Equivalents

Glenn Engelmann and Emmanuelle Trombe 12

Features

E-Discovery: Pre-Emptive Measures to Keep Costs Down

Terry Ahearn and William Brown 14

Al Capone's Downfall Is Still a Lesson: US Government Takes Tax Evasion Fight Worldwide

Todd Harrison 16

COMESA Competition Commission Publishes New Merger Assessment Guidelines

Carla Hine 18

Conversion to a German Company: An Option for EU Businesses

Clemens Just and Kian Tauser 20

Are No Hiring and No Poaching Agreements Enforceable in Germany?

Volker Teigelkötter and Bettina Holzberger 22

In This Issue

Welcome to the final issue of *International News* for 2014. As regulatory oversight of companies—from Sarbanes Oxley and the Dodd-Frank Act to the Foreign Corrupt Practices Act and the UK Bribery Act—becomes increasingly intrusive and complex, companies must continue to prioritise compliance. In this issue, therefore, we focus on some of the compliance challenges business face.

We start our Focus section by examining how one, uniform compliance programme can meet the global challenges faced by multinational companies.

It is also, of course, always best to prepare for the worst. The best approach to dealing with the complexities that can arise during an internal investigation is to have a well thought out internal investigation plan in place before a crisis hits. We outline how such a plan might look.

Even with a robust compliance programme and efficient internal investigation plan in place, companies sometimes face investigations from external bodies. Investigations into multinational companies that involve national authorities will also often trigger enquiries from the company's home country. We examine the key differences between Chinese and US styles of litigation to highlight the benefits of taking the most thorough approach while being sensitive to local practices.

Data protection rules affect every company, and create significant challenges when dealing with a number of regimes. For multinational organisations doing business on both sides of the Atlantic, the most successful compliance solution is to build a global data privacy program. We examine how that can be achieved.

Finally, we look at one of the most regulated sectors—health care— and the widely discussed topic of transparency in relation to gifts and transfers of value given by the pharmaceutical industry to health care professionals.

In our features section, we start with a look at keeping down costs during electronic discovery. The most expensive part of any document review process is the "eyes-on" review by lawyers. If you want to keep costs down, your ultimate goal is to minimise the number of irrelevant files that will need to be reviewed by your document review lawyers.

Tax evasion has become one of the top enforcement priorities of the US Government. We highlight the key lessons learned from recent aggressive, multi-pronged investigations by the US Department of Justice, the Internal Revenue Service and the US Senate.

The Common Market for Eastern and Southern Africa (COMESA) Competition Commission (CCC) published highly anticipated Merger Assessment Guidelines (Guidelines) on 31 October 2014. We summarise some of the key points of the Guidelines, which provide some much needed clarity to on the CCC's jurisdictional scope, when transactions must be notified to the supra-national competition authority and how the CCC will substantively assess mergers.

Cross-border transfers of companies into or out of Germany have, up until now, only been achieved as a cross-border merger. Case law now provides another option: companies may move from an EU Member State to Germany, or from Germany to another EU Member State, by means of a cross-border conversion. The key aspect of a conversion is the maintenance of the company's legal identity. Contracts and property rights continue and it is not necessary to transfer any contracts or assets.

Finally, and staying in Germany, we examine whether or not no poaching agreements and no hiring agreements are enforceable under German law.

If you have any comments on our articles or would like to discuss any of the issues raised, please contact me at hnineham@mwe.com.

Hugh Nineham
Partner & London Office Head
hnineham@mwe.com

How One Compliance Programme Can Meet Global Challenges

By **Karin Holloch** and **Neal White**

As regulatory oversight of companies—from Sarbanes Oxley and the Dodd-Frank Act to the Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act—becomes increasingly intrusive and complex, companies must focus on compliance. Failing to adopt preventive measures can, at best, result in time-consuming, expensive defences against accusations of misconduct and, at worst, in legal fines, penalties and public censure.

An effective compliance programme includes strong policies and procedures, education and reinforcement through training and certifications, and compliance auditing. Programmes must be tailored to the company's industry, global platform, business model, regulatory environment and culture.

Companies with global operations face special challenges in designing, implementing and enforcing company-wide compliance programmes. Languages are different; business practices will be different, especially if the international operations are part of recent acquisitions run by their former owners. Local managers may be totally unfamiliar with compliance programmes, especially if they are in non-Western countries, and they operate far from the eyes of the C-suite. Relationships with suppliers and customers can be long standing and difficult to change.

One Programme or Many?

Because of the far-reaching laws of a company's home country, and in order to install a company-wide culture of compliance, multinationals should consider developing a uniform programme that applies globally, rather than having separate country-by-country programmes.

To ensure implementation and enforcement, each country should ideally have its own responsible compliance officer who is high enough in the local management hierarchy to command the respect of the employees and the local management, and to enact disciplinary measures—up to termination if necessary—for noncompliance.

It is also advisable to define clear reporting lines. The Chief Compliance Officer has to make sure that he or she is being informed in case of significant noncompliance. If local management is involved, there should be no option for them to withhold such reports to headquarters.

To say that a company should have a global programme is not to say that doing so is easy. Companies designing, implementing and enforcing a global compliance programme must recognise the differences between countries and the kinds of risks inherent to doing business in particular countries, and assure that sufficient weight is given to them in the global programme.

A global compliance programme needs practical mechanisms that secure compliance through key policies. For example, the

screening process for hiring agents in foreign countries should be clearly defined and extensive procedures for ensuring compliance by intermediaries (especially in high risk countries) should be available. The internal control system should periodically review agent practices and agreements.

Communication and Training

Local implementation and enforcement may require local language versions of compliance programmes, both in written policies and live training. Some multinational companies have an official language in which business is to be conducted internally. Writing and teaching the compliance programme in that language may be appropriate as long as the workforce is sufficiently fluent in the official language to assure comprehension.

> Multinationals should consider developing a uniform programme that applies globally.

In some countries, such as France and Poland, internal work instructions have to be in the local language in order to bind the employees. In some cases, and particularly at levels of the workforce below management, the message cannot be effectively delivered unless local language is used.

Web-based training, while cost-efficient, may not be as effective as face-to-face training in some countries and at some levels of an organisation. While multiple translations will increase the cost of implementation, it will probably still be less than developing separate policies for subsidiaries around the world.

Whistleblowing

Companies with employees in more than one country should also ideally have a single whistleblowing reporting system, tailored to reflect local data protection laws and whistleblowing regulations. While EU Member States have greater data protection regulation than the United States, they do not protect whistleblowers to the same extent as the United States, unless the company takes extra steps to ensure protection.

For example, in Germany some companies appoint an internal or external ombudsperson to whom compliance concerns can be addressed live, rather than setting up a telephone hotline. In China, a whistleblowing system is vital as whistleblowing is frequently used to report noncompliance. To reduce communication barriers, whistleblowers should be able to report in their own language.

The Challenge of Gifts

The practice of gift giving in different countries presents a special challenge to drafting a global anti-corruption policy. The culture of giving gifts in Asia is totally different to the United States. A zero tolerance policy on gift giving and receiving requires sensitivity in order to be compliant with both Chinese traditions and Western anti-corruption laws.

Compliance is necessary not only for a company's own programme, but also to comply with covenants in contracts with public companies that require a company's foreign subsidiaries to have and enforce a programme that meets US or UK standards. Reputable Chinese businesses are encountering these requirements on a more regular basis as they do increasing volumes of business with Western companies, and so are becoming more familiar with them.

Local Law and the Long Arms of the FCPA and the UK Bribery Act

Although bribery and related corruption is forbidden in most countries, regulations may be less strict in countries outside the United States and the United Kingdom. Not all countries operate strictly on the rule of law. Even if the legal regulations in some countries are clear, they might not be enforced in day-to-day business.

The FCPA for the most part does not only not accept and legitimise those differences, but was specifically enacted to combat accepted local practices that conflict with US ethical standards. The UK Bribery Act is even more restrictive than the FCPA, *e.g.*, facilitation payments are not allowed under the UK Bribery Act.

There will be some risks and laws unique to a country that may have to receive special emphasis in the local implementation of a global programme. Identifying these local issues requires local expertise, so the local compliance managers and local lawyers should have input into the design of the programme. The compliance managers around the globe, as a group, should confer regularly to discuss local challenges and experiences in order to update and improve the programme. Conferring regularly will also reinforce their sense of working as team towards a common goal, and ally them as part of the global operation. Local laws have to be considered and monitored as they might set different standards for the organisation of compliance. Brazil and Russia have recently adopted anti-corruption laws that either require or encourage (by reducing penalties) the adoption of compliance management programmes laws. The German legislature currently has three different drafts under discussion.

> Not all countries operate strictly on the rule of law.

Additional Benefits

Creating and enforcing a global programme may also smooth the path of acquiring or divesting local operations. Acquirers and financing institutions will find comfort in the attention paid to compliance. Local compliance managers will be able to assist in the due diligence of new acquisitions and ease the extension of the acquirer's programme into the new operation. An effective global compliance management programme can therefore be a pillar of a successful expansion strategy.

Karin Holloch is a partner based in the Firm's Düsseldorf office. She co-leads the corporate department's compliance practice. Karin is a German-qualified lawyer specialising in preventive compliance, global compliance programmes and incident handling. Before joining McDermott, she was corporate counsel and head of international compliance of a world-leading retail company. Karin can be contacted on **+49 211 30211 113** or at **kholloch@mwe.com**.

Neal White is a senior partner based in the Firm's Chicago office. He co-leads the corporate department's compliance practice. In addition to compliance, Neal focuses his practice on business counselling, commercial law and finance with particular emphasis on acquisitions and divestitures, joint ventures and management/board relationships. He can be contacted on **+1 312 984 7579** or at **nwhite@mwe.com**.

Avoiding Common Pitfalls During Internal Investigations

By **Obiamaka Madubuko** and **Wolfgang Freiherr Raitz von Frentz**

Corporate counsel tasked with running an internal investigation face many challenges early on. ***What to investigate? Who should lead the investigation? Who to interview? Where are the relevant documents? How to stop the alleged misconduct? How much will this cost? Who do I need to tell?***

The pitfalls that can threaten in-house counsel's ability to manage the investigation to a successful conclusion are equally daunting: *How to protect privilege? What to do about differing local or international law requirements? How to deal with bad actors, whistle-blowers and government regulators?* The best approach to dealing with all the complexities that can arise during an internal investigation is to have a well thought out internal investigation plan in place before a crisis hits.

Problem 1: Managing Cost and Protecting Privilege

Do we even need an investigation? If so, I'm sure it will be more cost effective to handle it in-house.

An internal investigation plan should include an upfront assessment of the allegation to determine whether or not an investigation is needed and, if so, who should lead it. Sometimes, the claim is too vague to warrant an investigation. Other times the nature of the claim will require an in-depth investigation.

Sometimes outside counsel may be needed in order to protect privilege, particularly for international investigations where local laws shape what is considered attorney-client privilege or attorney work product. Companies may also want to leverage outside counsel's experience or to demonstrate independence to a regulator. If outside counsel is retained, determine whether or not regular or special outside counsel is needed and establish a budget upfront to help manage costs.

Claims should be quickly triaged and a system in place to ensure proper internal and external escalation to the necessary persons to address it.

Problem 2: Issuing Litigation Hold Notices

Who needs to know about the investigation? When is a litigation hold notice needed?

Always err on the side of caution and take appropriate steps to preserve evidence as soon as you receive notice of an issue that could give rise to a lawsuit. Issue a litigation hold notice promptly upon notice of a

potential claim and distribute it to anyone who may have relevant records. Include your IT department so they can take appropriate action, such as stopping or suspending auto-delete or over-write functions and preserving e-mail, backup tapes/servers, *etc.* to ensure all relevant documents have been preserved and workplace disruptions are minimised.

> A system should be in place to ensure proper internal and external escalation.

Failure to take appropriate action to preserve evidence can result in monetary fines, adverse jury instructions, preclusion of evidence, default judgment or dismissal (in a civil case) or obstruction charges (in a criminal case). To avoid potential obstruction or spoliation issues, reinforce company rules on document preservation in compliance manuals and through regular employee training.

Problem 3: Notifying the Board

Why bring an allegation to the general counsel's or board's attention before doing at least a preliminary investigation to see if it has any merit?

While the urge to keep the investigation to a "need to know" basis is the right one, several key factors need to be considered to determine who should be informed of an investigation and when. If an allegation is serious, *e.g.*, materially impacts the company's financials or its reputation, then it must be brought to the attention of the general counsel and board early on.

Conducting a preliminary investigation without getting the right guidance from in-house and/or external counsel can cause problems such as loss of privilege, loss of credibility from a regulator's perspective and violations of local law that are difficult to undo later. The general counsel and board should be kept apprised of possible litigation and enterprise risks, but their expectations can be managed by providing regular updates.

Problem 4: Disciplining Employees

What do we do if we suspect employee misconduct? Should we fire these employees immediately to show that we have a zero-tolerance policy against wrong-doing?

Suspicions of misconduct are different to having evidence of misconduct. The appropriate response will necessarily be fact-driven and will be decided on a case-by-case basis. It may be that the employee should not be fired before they have been interviewed by corporate counsel but should instead be put on administrative leave, with or without pay, until the investigation is further along and culpability levels can be fully assessed. Other times swift action may be appropriate.

Keep in mind, however, that whatever disciplinary action is taken, it should be done in consultation with employment counsel, human resources (HR) team members and the lead lawyers conducting the investigation.

HR should work closely with the legal and compliance departments to ensure that any reductions in the workforce that implicate possible whistle-blowers, material witnesses or others who may be involved in an investigation are vetted and discussed before such decisions are implemented.

Problem 5: Data Privacy and the Impact of Local Law

We need to interview our employees based in Europe and to review their documents as part of our internal investigation. I can't wait for them to agree to cooperate and I don't have time to waste going through European Works Councils now that US regulators are involved. If our employees do not cooperate, my view is that they should be fired.

Be wary of "threatening" to fire employees based outside the United States when conducting an internal investigation, as such "threats" may violate local laws and could create collateral damage for the company.

German law, for example, places certain restrictions on internal investigations, violations of which are subject to administrative fines or even criminal punishment. These restrictions may, for example, apply to e-mail searches. In addition, the consultation rights of the Works Council regarding internal investigations have to be respected. The Works Council, for example, has to be involved if employees are not individually interviewed but have to answer standardised questionnaires, or if the data collected in the investigation is processed in a database or by specific software. Additional participation or consultation rights may result from Works Council agreements.

When personal data is transferred from an EU country to a non-EU country, the EU rules on cross-border data transfer and processing apply, even if the data is transferred to and processed by an affiliated company. Such cross-border transfers then require the consent of all affected persons or the registration of the receiving party under Safe Harbor, EU Standard Clauses or a group-wide data protection scheme. The penalties for violating these procedures can subject the company and/or responsible persons to civil and/or criminal sanctions.

> Suspicions of misconduct are different to having evidence of misconduct.

Advance Planning

Internal investigations can be challenging given how many issues are involved and how each decision can trigger a whole new set of issues and concerns. Companies should therefore take the time to put appropriate protocols in place. By taking the steps outlined here, some of the more common legal problems that come up during an internal investigation can be spotted and stopped in advance.

Obiamaka Madubuko is a partner based in the Firm's New York office. She is co-chair of the Firm's Foreign Corrupt Practices Act & International Anti-Corruption Group and focuses her practice on anti-corruption and fraud matters, as well as advising US-based companies doing business in international markets. Obiamaka can be contacted on **+1 212 547 5308** or at **omadubuko@mwe.com**.

Wolfgang Freiherr Raitz von Frentz is a partner based in the Firm's Munich office. His practice is focused on commercial litigation and transactions and compliance. He coordinates and supervises in-house investigations by clients and develops and implements compliance programmes, in particular in the areas of anti-corruption, fraud and data protection. Wolfgang can be contacted on **+49 89 12712 157** or at **wfrentz@mwe.com**.

Defending Against Charges of Corruption in China: The Best of Chinese and US Styles

By **Ping An**

One afternoon in Shanghai, Joe Smith, an American lawyer new to China, was hired to represent the Chinese subsidiary (China Sub) of a multinational company (MNC) that was recently accused by the Chinese authorities of offering "kickbacks" to procurement specialists at a PRC state-owned enterprise (SOE) in an attempt to induce the SOE's employees to purchase China Sub's products rather than its competitors'. As the United States Department of Justice (DOJ) closely monitors developments in China, it swiftly sent a letter to the MNC's general counsel asking for an explanation.

Joe's first task was to accompany China Sub's chief compliance officer to his interview with officers from the Shanghai Municipal Bureau of Public Security, which was handling the investigation. The officers stopped Joe from entering the interrogation room and inquired who he was and why he was there. Upon hearing Joe was a lawyer representing China Sub, the officer-in-charge told Joe he did not need to be there as all cases are handled with fairness and transparency. Joe made it clear that he was entitled to be there because his client had requested counsel to be present during all adversarial legal proceedings. Joe's reply drew an incredulous look from the officers in the room and a swift rebuke from the officer in charge.

Although this scenario is fictional, the lessons are not. US lawyers and Chinese local practitioners frequently run into problems over cultural differences and fundamentally opposed approaches to litigation and government investigation, which can make investigating and defending corruption charges involving businesses active in China very difficult.

The Importance of Facts

US litigators are trained to focus on the facts of the case and craft legal arguments and legal strategies based on those facts. US lawyers are trained to presume nothing and verify every detail, even ones that would at

first glance appear trivial. As a result, the fact-finding processes in US litigations are usually very thorough and comprehensive.

Typically, the Chinese litigation style is different. Some Chinese lawyers are not accustomed to asking questions thoroughly, are reluctant to ask questions that can be perceived as being rude and, in general, pay less attention to detail than required of their US counterparts.

> It is common to find testimonies that are exaggerated, half true or just plain false.

One of the reasons for this is cultural: Chinese society emphasises indirect communication. Some forms of direct questioning are perceived to be overly confrontational and therefore rude. Another reason is due to the many grey areas of law regulating Chinese business operations. For example, some actions prevalent in Chinese business practices often seem to be prohibited by law (or by the strict meaning of the law), and the concern is that asking too many questions will only create problems for the company.

Although this means it may prove difficult to uncover the facts of a case, it is important that these cultural differences are overcome. The facts are effective in defending against both charges raised by the Chinese authorities and potential subsequent Foreign Corrupt Practices Act (FCPA) investigations. Discovery in China should therefore be on par with US discovery protocol. Avoiding asking difficult questions is not an option.

At the same time, however, local Chinese expertise is invaluable. Few US lawyers speak, much less read or write Chinese. Because of the differences in culture, US lawyers need the guidance of Chinese lawyers to identify the local loopholes that allow an MNC's lower employees to engage in activities that violate the FCPA.

The best solution, therefore, is to work with a team comprising both Chinese local counsel and US litigators.

Key Differences

Notes taken at interviews are not always complete and will rely too much on the lawyers' memories. Most Chinese lawyers, however, prefer to take notes without recording the interviewee for fear that the interviewee will be less forthcoming if he or she thinks the interview will be recorded.

PRC law does not require the subject of the interview to be apprised that the conversation will be recorded, whereas in the United States, best practice dictates that the interviewee is advised they are being recorded to ensure there are no subsequent challenges to the authenticity of the recording. Furthermore, MNCs that place great emphasis on internal investigation procedures may have qualms about not disclosing every detail to the interviewee. After taking advice from both Chinese and US counsel, the MNC must decide whether or not to tape interviews.

> Chinese society emphasises indirect communication.

US evidence codes (such as the Federal Rules of Evidence) and deposition procedures highlight a key difference between the United States and China. Prior to making a deposition in the United States, the party deposed has to swear an oath and is made aware of the requirement to tell the truth. He or she is also accompanied by counsel, who should have explained the deposition process beforehand and may object to the form of questions during deposition if necessary.

The same is not, and cannot be, done in China. It is common to find testimonies that are exaggerated, half true or just plain false. It is therefore vital to keep US evidentiary standards in mind while conducting deposition interviews in China. For example, if an employee says, "He told me he used to forge receipts through fictitious travel agencies to funnel kickbacks to the guy in charge of procurement at SOE", counsel should probe at the foundation of the employee's statement. Something as simple as "How do you know he actually did that?" can go a long way towards separating fact from fiction.

The Impact on Electronic Discovery of Chinese State Secrets and Trade Secrets Law

The Guarding State Secrets Law of the People's Republic of China (the Law) prohibits illegally obtaining state secrets, transferring state secrets through the internet without safeguarding measures or exporting state secrets abroad without permission. The Law defines state secrets broadly as "Matters that have a vital bearing on state security and national interests and, as specified by legal procedure, are entrusted to a limited number of people for a given period of time."

Chinese commercial/trade secrets are protected by the Anti-Unfair Competition Law of 1993 and the Central Enterprises Trade Secret Protection Interim Provisions (the Interim Provisions) issued in 2010. The Interim Provisions provide that a trade secret may be upgraded to a state secret, provided that statutory procedures for determining state secrets have been undertaken. Practically speaking, almost any non-publicly available information in China can be classified as trade secrets and potentially upgraded to state secrets. This means any information obtained during discovery that is not readily available publicly in China could be considered a trade secret and, possibly, a state secret.

As a result, it is advisable for international law firms and MNCs to have a separate data collection centre in China (for the purpose of Chinese state secrets law, Hong Kong is considered a foreign jurisdiction) and have knowledgeable staff screen all information before releasing the information overseas.

FCPA investigations and defence are inherently difficult. Adding the additional China dimension, with all its language, cultural and legal differences, can make even a seasoned litigator lose sleep. But working with trusted Chinese local counsel who have ample US litigation experience, supported by a competent local electronic discovery team, will help maximise your chances of success.

Ping An is foreign counsel for MWE China Law Offices in Shanghai, where he focuses his practice on corporate compliance and government investigation issues. Ping can be contacted on **+8621 6105 0500** or at **pan@mwechinalaw.com**.

EU and US Data Protection Standards – Finding Common Ground

By **Rohan Massey** and **Heather Egan Sussman**

The United States and the European Union take different approaches to privacy and data protection, each strict in its own way. For multinational organisations doing business on both sides of the Atlantic, the most successful compliance solution is to build a global data privacy programme that acknowledges the differences, builds on the similarities and finds common privacy ground.

Europe

The EU "omnibus" regime focuses its regulatory efforts on protecting any information that can be used to identify a living person (personal data), regardless of business sector or activity. The core of the regime is the protection of the individual (data subject), who has a fundamental right to know who is collecting, accessing, using, storing, transferring and deleting (processing) his or her personal data, and what it is being used for. For entities processing personal data in the European Union, the relevant data protection laws require implementation of minimum security measures designed to protect the data from unauthorised use or access, to retain data for no longer than necessary and to provide an individual, upon request, with information regarding any personal data held by the entity.

The European Union prohibits the transfer of EU citizens' personal data to countries outside the European Union or the European Economic Area (EEA) unless the data is adequately protected. Notably, the European Union does not recognise the United States as giving adequate protection.

The United States

The US "sectoral" regime emphasises regulation of certain industries, business activities and types of sensitive personal data that generate an increased risk of harm to the individual. For example, a number of US federal laws impose strict requirements on specific industries, *e.g.*, the government, financial services and health care sectors, and the service providers doing business with those sectors, and a complex web of federal and state laws regulating business activities that create risk for the individual.

In addition to these laws, 12 US states require entities processing "personal information" to implement reasonable administrative, physical and technical safeguards designed to protect such information. Generally, these laws define personal information to include name, plus any other data element that could create a greater risk of harm to the individual if wrongfully disclosed or misused.

These business-, activity- and information-specific laws are supplemented by state and federal consumer protection laws that, when taken together, provide broad coverage over most businesses in the United States.

Global Trends

Over the past decade, an increasing number of countries around the world have adopted an EU-style omnibus regime. A main driver for this is a country's desire for an EU adequate protection finding in order to facilitate data transfers—and thus trade—with the European Union. It is, however, questionable whether or not some of these jurisdictions have the capability to actually enforce the laws they impose because they lack sufficiently robust data protection authorities experienced in this area.

In contrast, in the United States, between the dozens of fully staffed federal agencies with specifically granted enforcement authority, and each state's own attorney general responsible for enforcing state privacy laws through the separately state-funded office, companies doing business in the United States face the constant risk of sophisticated, coordinated, robust, multi-agency enforcement action following privacy and security missteps. These risks are increasingly driving US corporate boards of directors to demand best-in-class global data privacy and security programmes to reduce the risk of litigation and enforcement action in the United States.

Although EU regulators are still reluctant to find interoperability between the EU and US approaches, for multinationals caught in a battle of regulators there is actually a pathway to common ground.

Finding Common Ground

The way forward is to build a global data privacy programme based on the FIPPs (see box) that were first articulated by the Organisation for Economic Co-operation and Development in 1981, and layer into the programme specific regulatory requirements imposed by the jurisdictions in which the company operates by following these important steps.

Implement an Effective Governance Structure: This includes designating one or more individuals to oversee the design, implementation and administration of the programme. In most large, multinational organisations, the designated individuals report up through appropriate senior or board level to ensure accountability.

Deploy Safeguards: Design and implement reasonable administrative, physical and technical safeguards designed to protect the data processed by the organization. The safeguards should be appropriate to the size and scope of the organization, the sensitivity of the data processed, as well as the particular risks to the data at issue.

Consider Specific Jurisdictional Requirements: Supplement the general FIPPs with jurisdiction-specific regulatory requirements. To do this, the organisation needs to consider how to incorporate stricter requirements from a particular jurisdiction into a global platform.

Design a Data Transfer Solution: Before determining what is the appropriate solution for legitimising transfers of data outside of the EU and elsewhere with similar laws, entities must assess their requirements: what data is being transferred, why is it being transferred, where is it being transferred from, is it all internal to the business or are third parties involved? Once these questions are answered, options for the most suitable solution can be considered, taking into account the entity's risk profile and commercial factors, such as cost, length of time to implement and regulatory involvement in the process.

Robust Vendor Management Programme: Determine what third parties (vendors and business partners) have access to (1) the organisation's network or technology infrastructure, *e.g.*, technology consultants; (2) its premises, *e.g.*, delivery persons; or (3) the personal data itself, *e.g.*, shredding companies. The programme should ensure minimum contractual provisions are in place with such third parties, and procedures for conducting effective due diligence to ensure these third parties are capable of maintaining the security of the systems, premises and personal data to which they have access.

Put It in Writing: One of the first documents requested by a regulator during an investigation is a copy of the company's written programme. Companies that cannot produce a written document are viewed as deficient, which sets the tone for an ensuing investigation.

Ensure Ongoing Monitoring and Review of the Programme: It is not sufficient merely to document data privacy and protection agreements and policies; they must be fully and effectively implemented and adhered to on an ongoing basis. They must be made clear to current personnel and newly hired employees through a robust and ongoing training programme. Employees need to be made aware of the applicable impact on their behaviour, the obligations placed on them by the law and the consequences of non-compliance, both legally and in relation to their employment. After a programme has been rolled out to the organisation, it needs to be refreshed as appropriate to remain functional and adapted to reflect changes in business practices.

The Eight Fair Information Practice Principles (FIPP)

The FIPPs underlie the EU data protection regime, a number of the sector-specific US federal laws regulating privacy and data security, and certain published guidance from the Federal Trade Commission and other US agencies in the areas of privacy and data security.

1. **Collection Limitation:** The collection of personal data should be limited; they should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. **Data Quality:** Personal data should be relevant to the purposes for which they are to be used; they should be accurate, complete and kept up-to-date to the extent necessary for those purposes.
3. **Purpose Specification:** The purposes for which personal data are collected should be specified at the time of collection and their use limited to the fulfilment of those purposes, or others not incompatible with those purposes, and specified each time the purpose is changed.
4. **Use Limitation:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except with the consent of the data subject or by the authority of law.
5. **Security Safeguards:** Personal data should be protected by reasonable security safeguards against risks, *e.g.*, loss or unauthorised access, destruction, misuse, modification or disclosure.
6. **Openness:** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. **Individual Participation:** An individual should have the right:
   a) To obtain from a data controller confirmation of whether or not the data controller holds data relating to him or her
   b) To have communicated to him or her within a reasonable time, data relating to him or her at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him or her
   c) To be given reasons if a request for information about personal data is denied, and to be able to challenge that denial
   d) To challenge data relating to him or her and, if the challenge is successful, to have the data erased, rectified, completed or amended
8. **Accountability:** A data controller should be accountable for complying with measures that implement the eight principles.

Conclusion

Under proposed regulation under consideration in Europe, regulators may be given the power to fine up to 5 per cent of global turnover. By following the steps above, however, it is possible to find common ground among the competing privacy and data protection regimes around the world, in a way that mitigates risk to the company, to the data and to the individuals these laws are designed to protect.

Rohan Massey is a partner based in the Firm's London office. He is the head of the intellectual property, media & technology practice in London and focuses his practice on media, e-commerce, outsourcing, IT and data protection. Rohan can be contacted on **+44 20 7577 6929** or at **rmassey@mwe.com**.

Heather Egan Sussman is a partner based in the Firm's Boston office. She is Co-Chair of the firm's global privacy and data protection affinity group and is a Certified Information Privacy Professional. Heather can be contacted on **+1 617 535 4177** or at **hsussman@mwe.com**.

Disclosure Requirements in the Health Care Sector: The Sunshine Act and Its European Equivalents

By **Glenn Engelmann** and **Emmanuelle Trombe**

The pharmaceutical industry has traditionally fostered a range of relationships with health care professionals (HCPs) in connection with the development and sale of medical devices and prescription-only medicines. Some of these relationships involve value exchanges, which can include payment for services rendered or, in some cases gifts, and are often considered to have the potential to create conflicts of interest.

United States

A universal transparency requirement was introduced with the enactment of the so-called Sunshine Provisions or Sunshine Act as part of the Affordable Care Act in 2010. The explicit goal of the legislation was to increase transparency in financial relationships between industry and group purchasing organisations, and physicians and teaching hospitals.

Summary of the Law's Requirements

An "Applicable Manufacturer", which must report financial data, is defined in the legislation as an entity that is operating in the United States and is either

- Engaged in the production, preparation, propagation, compounding or conversion of a covered drug, device, biological or medical supply
- An entity under common ownership with a manufacturer that provides assistance or support in production, preparation, propagation, compounding, conversion, marketing, promotion, sale or distribution

The Centers for Medicare & Medicaid Services (CMS) set the common ownership bar quite low (5 per cent) with respect to entities within a corporate family.

While there are some exclusions, an entity that holds a Federal Drug Administration (FDA) approved license or clearance for a "Covered Product" manufactured or marketed in the United States is obligated to report. A Covered Product is one that is available under the Social Security Act (SSA), Title XVIII (Medicare D or a State Plan under Title XIX (Medicaid)) or Title XXI (CHIP). Over-the-counter drugs and biologicals, plus devices and medical supplies not requiring pre-market approval are not covered. The regulations allow for a 180-day grace period after a first product is covered before compliance with the reporting requirements of the law becomes mandatory.

In general, once an entity meets the definition of Applicable Manufacturer, all payments or transfers of value, regardless of whether or not they relate to a Covered Product, must be reported.

"Covered Recipients" include physicians, dentists, podiatrists, optometrists and chiropractors, group purchasing

organisations and teaching hospitals. There are 16 categories of payments that must be reported, with 14 exclusions, including exclusions for product samples, certain loans of covered devices, warranties, discounts and rebates. Both direct and indirect payments are reportable.

Special provisions, templates and guidance exist for research-related activities. The total amount spent in connection with the research project needs to be reported. Segregable activities can, however, be reported separately and payments to non-covered recipients that are not passed on to Covered Recipients are excluded.

Applicable Manufacturers must register with CMS before submitting their financial data. Delayed publication may be requested for payments made under a product development agreement and clinical investigations. Payments made by separate entities under common ownership with an Applicable Manufacturer may be consolidated. Joint venture partners may specify which partner files, but in the absence of an agreement, the party making the payment must report.

Applicable Manufacturers have 45 days to resolve any dispute with Covered Recipients. Without agreement, the manufacturer's view will be reported. Corrections may be made at a later date, but the corrected information will not be publicly available until the next reporting cycle.

Europe

Because transparency requirements are not harmonised across the EU Member States, a number of States have adopted rules similar to the Sunshine Act, or strengthened pre-existing regulation. In parallel with these national rules, conventional standards have been set by the European Federation of Pharmaceutical Industries and Associations (EFPIA).

Requirements of the EFPIA Code

To avoid conflicts arising, in 2007 the EFPIA adopted two Codes to ensure that interactions between HCPs and the pharmaceutical industry meet the high standards of integrity that patients, governments and other stakeholders expect:

- The Code on the Promotion of Prescription Only Medicines to Healthcare Professionals
- The Code of Practice on Relationships between the Pharmaceutical Industry and Patient Organisations

On 24 June 2013 the EFPIA Board also adopted a Code on Disclosure of Transfers of Value from Pharmaceutical Companies to HCPs and Healthcare Organisations (HCOs) (the Disclosure Code) which refers only to prescription drugs. The Disclosure Code applies to EFPIA Member Companies, including

- Corporate members: research-based pharmaceutical companies that develop and manufacture medicinal products in Europe for human use.
- Affiliate members: companies specialising in particular fields of pharmaceutical research and/or development or in new technologies of particular interest to the pharmaceutical industry.
- Research-based pharmaceutical companies operating in a particular segment of the pharmaceutical market, *e.g.*, European Biopharmaceutical Enterprises and Vaccines Europe.

Each Member Company must disclose direct and indirect transfers of value relating to prescription drugs to, or for the benefit of, HCPs or HCOs within six months of the end of a relevant reporting period. The first reporting period is the calendar year 2015, with disclosure required in July 2016.

The categories of value transfers to be disclosed are contributions to costs related to events and fees for services, consultancy fees and donations and grants. The disclosure must clearly identify the recipient and the amount.

Each Member Company has to document and disclose on its website, or on a common website, the names of HCOs, HCPs and associations that have received payments or other transfers of value, the amounts and the category of relationship.

France

In 2011, France adopted Law No. 2011-2012 on the Strengthening of Health Protection for Medicinal and Health Products. The scope of this legislation is broader than the EFPIA Code as it applies to almost all participants in the health care industry: not only pharmaceutical companies, but also medical device manufacturers, Contract Research Organisations, communication agencies and consultants. They are required to disclose agreements entered into with HCPs and HCOs, and advantages in kind or in cash exceeding €10, provided directly or indirectly to HCPs and HCOs.

The level of disclosure, however, may be less specific than the EFPIA Code, as only advantages in kind or in cash must be disclosed, and not fees or other compensations.

Companies that knowingly fail to fulfil the obligation to publicly disclose face a fine and sanctions.

The United Kingdom

Some Member States do not have an equivalent to the Sunshine Legislation and instead rely on professional codes.

The UK health care self-regulatory system consists mainly of the Association of the British Pharmaceutical Industry (ABPI), the Proprietary Association of Great Britain and the Association of British Healthcare Industries, which have all published codes of good practice. The most comprehensive on transparency is the ABPI's. Sanctions for breaching the ABPI Code include public reprimand and/or suspension or expulsion from membership of the ABPI.

In addition, under the UK Bribery Act 2010, a company must be able to show that it had "adequate procedures" in place to prevent persons associated with it from bribing. Compliance with the ABPI Code is likely to be taken into account when assessing whether or not those procedures were adequate.

Claire Manouvriez, a trainee based in the Firm's Paris office, and Camille Spegt, a stagiaire based in the Firm's Paris office, also contributed to this article.

Glenn Engelmann is senior counsel based in the Firm's Washington, DC, office. He is vice chair of the Firm's Life Sciences Industry Group and has 25 years of experience managing complex legal and regulatory matters in the pharmaceutical industry. Glenn can be contacted on **+1 202 756 8388** or at **gengelmann@mwe.com**.

Emmanuelle Trombe is a partner based in the Firm's Paris office and a member of the Corporate Advisory Practice Group. She focuses on the pharmaceutical, medical device and health care industries. Emmanuelle can be contacted on **+33 1 81 69 15 35** or at **etrombe@mwe.com**.

E-Discovery: Pre-Emptive Measures to Keep Costs Down

By **Terry Ahearn** and **William Brown**

The most expensive part of any document review process is the "eyes-on" review by lawyers. If you want to keep costs down, your ultimate goal is to minimise the number of irrelevant files that will need to be reviewed by your document review lawyers.

Most of the files that can easily be excluded from document collection fall into three categories: unnecessary e-mails, photos and duplicates. By following a few simple rules, you can prevent your electronic documents, and therefore your e-discovery budget, from spiraling out of control.

E-Mail Management

Keep Personal E-Mails Out of the Corporate E-Mail System

Your corporate e-mail policy may strictly prohibit the use of corporate e-mail for personal use, or allow but discourage the use of corporate e-mail for personal use. A policy is, however, of no use if it is not enforced consistently. Is yours, for example, enforced against your high-level corporate superstars? When setting the policy on the use of e-mail for personal matters, consider allowing the use on work devices of personal web-based e-mail for personal e-mails, so office e-mail is reserved for work only. Otherwise, when your company is in a lawsuit, e-mails discussing childcare plans, vacations, romantic *rendezvous*, investment portfolios, politics, tax returns, divorce proceedings and other irrelevant topics may need to be opened, reviewed and coded, costing you time and money.

To ensure compliance, it may help to remind your employees, including executives, that each personal message they receive or send may get opened and reviewed by your lawyers. If concern about wasting corporate funds doesn't help them adhere to your

policy, the fact that personal e-mails may be read by an outsider might do the trick.

Keep Work E-Mails Out of Personal E-mail Accounts

The flip side is to discourage the use of personal e-mail accounts for work. Personal e-mail might be used if a work e-mail system is not accessible by the employee when away from the office on business. Such use may subject the employee's private e-mail accounts to the same litigation holds, collection and review as office e-mail. This can add a lot of data to your collection and significant uncertainty when determining whether or not relevant e-mails have been retained. If the use of personal e-mail is unavoidable, encourage the use of sensible folders or labels to keep work-related e-mails segregated.

Photographs

Unlike e-mails and electronic documents, photos cannot be filtered or searched based on their content. When faced with thousands of photographs with filenames like "Imagexxxxxxx.jpg", reviewers may have no choice but to open and examine each one. On some cases reviewers have spent large amounts of time sifting through thousands of photos from vacations, weddings, graduations, sports games and birthday parties while trying to locate potentially relevant photos.

> Reviewers have seen single PowerPoint files with 80 embedded documents.

Clearly named folders can help identify photos that may be relevant ("New Product Test") and eliminate others that are not ("Office Summer Party"). It also helps to have in place policies that make it clear that personal photos should not be stored on work devices. When a personal device is used for work photos, make sure the employee knows how to load only the work photos to the work computer and that they must immediately delete any personal photos uploaded accidentally.

Duplicates

Attachments

If your company uses a document management system, you probably have the ability to send either a link to a document or the document itself. Set the default to the link. Otherwise, when the document is passed back and forth on various e-mails, the file is being duplicated, which increases the number of documents to be reviewed. The same scheme can be used with cloud storage: circulate the link, not a copy of the file.

Embedded Documents

An embedded document is a file tucked within another file. A common example is a chart or table from an Excel file placed into a Word or PowerPoint file. Depending on how the author added the information from the second file, it may embed the whole second file, rather than just the chart or table.

Reviewers have seen single PowerPoint files with 80 embedded documents. Sometimes the same workbook will be embedded several times in a document and will need to be opened, reviewed and coded each time. When the main document is revised and recirculated, the same or a similar set of embedded documents are circulated again. If someone adds a few more, the number increases exponentially.

If your organisation does embed documents in this way, be sure to discuss this with your litigation or discovery counsel at the start of the collection phase. You should also consider a joint stipulation with the other side on how to deal with embedded documents. For example, the parties could agree that all embedded documents will be extracted before production, or that embedded documents will only be extracted upon request.

Avoid Extra Copies

If your computer systems are unreliable, good, hard-working employees will start creating workarounds that result in multiple copies of each document. For example, if your company's document management system is hard to use, or if it has a reputation for crashing, employees will start saving extra "just-in-case" copies on local hard disks or on other servers such as "home" directories (not to mention hard copies). Now you have more duplicates, near-duplicates and additional sources of discoverable information to track and search.

Why Can't I Just De-Dupe My Collection?

You may think that you don't need to worry about duplicates, because every vendor can de-duplicate, so reviewers will only look at one, or a few copies, at most. You would be wrong. For exact duplicate detection, the files have to have exactly the same content. Even if nothing more than a single space is added when a file is opened, the file becomes a distinct and different file. Word and PDF versions of the same document may print the same, but will not be considered duplicates by the computer.

> As forwards and replies multiply, so do the number of copies of the common attachment.

Another issue with de-duplication is de-duplication by family. E-mail A, with attachment X, is a simple document family. E-mail B, a forward of A, with attachment X, is another family. Attachment X will be in the document population twice, and therefore not eliminated by a de-duping exercise, because it is part of two different families. As forwards and replies multiply, so do the number of copies of the common attachment.

A final word of caution. If you are currently under a litigation hold, you must seek the advice of your counsel before deleting anything. There is, however, nothing to stop you from following these guidelines during the course of normal business and helping yourself to reduce the number of documents that could potentially waste your time and money during a dispute.

Terry Ahearn is a partner based in the Firm's Silicon Valley office. His practice includes intellectual property litigation and other complex commercial litigation related to high technology. Terry has significant experience in managing large-scale discovery. He can be contacted on **+1 650 815 7424** or at **tahearn@mwe.com**.

William Brown is a staff attorney based in the Firm's Silicon Valley office. His practice is focused on electronic discovery in intellectual property and general business matters. William can be contacted at **+1 650 815 7420** or at **wrbrown@mwe.com**.

Al Capone's Downfall Is Still a Lesson: US Government Takes Tax Evasion Fight Worldwide

By **Todd Harrison**

In the 1920s, Al "Scarface" Capone committed a lengthy list of substantial crimes, from homicides carried out at his behest to the manner in which he accumulated his US$100 million fortune. Ultimately, Capone was sentenced to 11 years in prison; not for money laundering or homicide, but for simple tax evasion.

Eight decades later, Al Capone should be on the mind of virtually every financial institution in the world, particularly those with US accounts held by US citizens or legal residents (US persons). This is because tax evasion has become one of the top enforcement priorities of the US Government. In recent years, US authorities have hammered Swiss financial institutions with stiff penalties for providing offshore tax shelters to US persons, most notably UBS in 2009 and Credit Suisse in 2014. These banks have been the subject of aggressive, multi-pronged investigations from the US Department of Justice (DOJ), the Internal Revenue Service (IRS) and the US Senate.

Anti-tax evasion efforts are no longer confined to Switzerland. Encouraged by the UBS and Credit Suisse penalties—and armed with new legal weapons—the DOJ has pledged to investigate offshore US accounts around the world.

Historical Overview

UBS Investigation

Recent US anti-tax evasion efforts began with the investigation of UBS, Switzerland's largest bank. In 2005, former employee Bradley Birkenfeld disclosed to US authorities the manner in which UBS was allegedly giving illegal tax-sheltering advice to clients. Birkenfeld's disclosures formed the basis of a massive US investigation of alleged tax sheltering of accounts held by US persons.

Around 2008, the US Senate Permanent Subcommittee on Investigations (PSI) launched its own investigation of UBS and LGT Bank in Lichtenstein, culminating in the release of a 110-page report detailing how the institutions were allegedly assisting US taxpayers to evade taxes by "Structuring [their] accounts to avoid disclosure to US authorities." The PSI held public hearings with UBS executives and US Government officials, building public support for anti-tax evasion legislation and exerting political pressure on the DOJ and IRS to extract penalties from violators.

UBS cooperated extensively with US investigators, the first time in several hundred years of Swiss banking that a Swiss bank had done so. In so doing, UBS was able to avoid a criminal conviction, receiving instead a deferred prosecution agreement and US$780 million fine.

The biggest win for the United States under the settlement agreement came as UBS released data on more than 4,000 accounts. This was only possible after the Swiss Government enacted emergency powers allowing UBS to disclose the names of account holders. Birkenfeld was prosecuted and sentenced to 40 months in prison but received a US$100 million payment from the US Government—the largest whistleblower award in history—thereby ensuring that more whistleblowers will step forward in the future.

As a result of the UBS settlement, new tax information-sharing treaties were signed between the United States and various countries. In 2009, the G20 nations proclaimed that the "Era of bank secrecy is over." Under the IRS's Voluntary Disclosure Program, tens of thousands of Americans began voluntarily disclosing their offshore accounts to the IRS in exchange for reduced penalties. Then, a second Swiss financial giant found itself in the crosshairs.

Credit Suisse Investigation

After the UBS settlement, the PSI and DOJ ran parallel investigations into Credit Suisse. In 2008, the PSI began asking Credit Suisse and other Swiss banks about their offshore tax account practices. In 2011, the DOJ indicted seven Credit Suisse employees for conspiracy to defraud the United States.

In early 2014, the PSI released a major report (176 pages) on offshore tax sheltering at Credit Suisse, claiming that Credit Suisse was dragging its feet in uncovering and exiting the problematic accounts. The PSI held public hearings but, this time, it also focused its ire on the DOJ, asserting that the DOJ too easily let Swiss banks avoid giving up client names by allowing them to hide behind Switzerland's bank secrecy laws. Since 2008, the DOJ "Obtained information, including US client names, for only 238 undeclared Swiss accounts out of the tens of thousands opened offshore," according to Senator Carl Levin.

The PSI's unparalleled ability among US investigators to rally political pressure was successful. Just three months after the hearings, Credit Suisse became the first bank to plead guilty to a US crime in more than a decade, a "sign that banking giants are no longer immune from criminal charges," according to *The New York Times*. Credit Suisse paid a staggering US$2.8 billion in fines to various US agencies and the New York State Department of Financial Services.

> "Tax evasion has become one of the top enforcement priorities of the US Government."

Key Lessons

Lesson 1: FATCA Takes US Anti-Tax Evasion Efforts Worldwide

The DOJ's aggressive efforts to fight tax evasion are now going worldwide, and the law leaves little choice other than to comply. In 2010, President Obama signed the Foreign Account Tax Compliance Act (FATCA), which compels certain US taxpayers to fill out forms providing details on overseas financial accounts or face a US$10,000, or greater, fine. Moreover, FATCA requires financial institutions outside the United States to report US account holders or be subject to a penalty on income earned from US sources. According to *Forbes*, more than 80 nations and more than 77,000 financial institutions have agreed to comply with FATCA.

Lesson 2: Do Not Assume Any Company Is "Too Big to Jail"

Since the financial crisis, the DOJ has come under fire from the American public for entering into settlements with financial institutions instead of seeking convictions of executives and institutions. The DOJ had been reluctant to indict or convict a systemically significant financial institution because of the potential risk to the global economy. The DOJ, however, essentially forced Credit Suisse to plead guilty by seeking assurances from US regulators that the bank's charter and licenses would not be revoked, blunting negative impacts to the economy resulting from the plea. Accordingly, banks across the world can no longer assume that they can settle with the DOJ with a solely financial penalty and avoid pleading guilty to criminal charges. Nor, on the other hand, can less systemically significant institutions assume that the United States will safeguard their charter in the event of a plea. "This case shows that no financial institution, no matter its size or global reach, is above the law," said US Attorney General Eric Holder regarding the Credit Suisse plea.

Lesson 3: Cooperation Is Key

All financial institutions of any significant size must be able to operate in the United States and conduct transactions in US dollars. With the threat of revoking a bank's charter or otherwise ending a bank's ability to operate in the United States, even through correspondent accounts, the US Government has the ultimate weapon to ensure compliance.

FATCA imposes hefty penalties for a failure to cooperate with reporting obligations. Not surprisingly, the Swiss operations of Deutsche Bank, Morgan Stanley and Goldman Sachs have publicly disclosed their cooperation with a DOJ self-reporting program, according to *The Wall Street Journal*, and about 40,000 individuals have disclosed their offshore accounts to the IRS Voluntary Disclosure Program.

The US Government will seek to punish the entities they view as non-cooperative. It is no coincidence that Credit Suisse—which the US Government claimed "allowed evidence to be lost or destroyed"—paid US$2.8 billion in fines and pled guilty. UBS on the other hand—which the US Government saw as more cooperative—received a deferred prosecution agreement and only paid US$780 million.

Todd Harrison is a partner based in the Firm's New York office. He focuses his practice on white-collar and corporate defense, internal investigations, regulatory and compliance matters, and complex civil litigation in state and federal courts. Todd has represented numerous companies facing government investigations, prosecutions and enforcement actions. He can be contacted on **+1 212 547 5727** or at **tdharrison@mwe.com**.

COMESA Competition Commission Publishes New Merger Assessment Guidelines

By **Carla Hine**

The Common Market for Eastern and Southern Africa (COMESA) Competition Commission (CCC) published highly anticipated Merger Assessment Guidelines (Guidelines) on 31 October 2014. The Guidelines provide some much needed clarity on the CCC's jurisdictional scope and when transactions must be notified to the supra-national competition authority, as well as how the CCC will substantively assess mergers.

COMESA Member States include Burundi, Comoros, the Democratic Republic of the Congo, Djibouti, Egypt, Eritrea, Ethiopia, Kenya, Libya, Madagascar, Malawi (where COMESA is based), Mauritius, Rwanda, Seychelles, Sudan, Swaziland, Uganda, Zambia and Zimbabwe.

Jurisdictional Thresholds

As reported in "Understanding the COMESA Merger Control Regime" (*International News*, Issue 2, 2014), COMESA's competition regulations apply to

> *The direct or indirect acquisition or establishment of a controlling interest by one or more persons in the whole or part of a business, where both the acquiring firm and target firm operate in two or more Member States and where the relevant turnover or asset threshold has been exceeded*

A "controlling interest" may be achieved through the purchase of shares or assets, or through some other amalgamation or combination, including "full-function" joint ventures, which do not include joint ventures that simply take over one specific function of a business, such as research and development. Acquisitions of assets are only reportable if the assets comprise a business with a market presence to which turnover can be clearly attributed.

Similar to the approach taken in the European Union, the Guidelines describe "control" as having rights that "confer the possibility of exercising decisive influence." Among the factors that may evidence "decisive influence", the CCC will consider whether or not the party

- Can determine a majority of the votes that can be cast at a general meeting of the undertaking
- Is able to appoint or to veto the appointment of a majority of the directors of the undertaking

- Can appoint senior management or determine commercial strategies, the budget or the business plan of an undertaking
- Has a controlling interest in an entity that in turn has a controlling interest in the undertaking

The Guidelines further clarify that non-voting securities, or a passive investment of less than 15 per cent of the voting securities, of an undertaking are not reportable.

The thresholds in the COMESA Competition Regulations (Regulations) are set at zero, but transactions are caught if they have an appreciable effect on trade between COMESA Member States and restrict competition in the COMESA Common Market. While the Regulations' thresholds have not been amended—this can only be done by the COMESA Council of Ministers—the Guidelines clarify that a merger must be notified if

- At least one party has turnover in excess of US$5 million in each of two or more COMESA Member States
- The target has turnover in excess of US$5 million in one or more COMESA Member States
- Not more than two-thirds of the annual turnover in the Common Market of each of the parties is achieved or held within one and the same Member State

Deadlines for Filing and a CCC Decision

If a transaction is subject to CCC review, the parties must notify it to the CCC within 30 days of their decision to merge. The Guidelines clarify that a "decision to merge" refers to the signing of "a definitive, legally binding agreement", or the announcement of a public bid for publicly traded securities. For the purposes of the 30-day deadline, parties that submit filings as per the Guidelines will be considered compliant, even if the CCC later deems that the filing was incomplete. Unlike many other jurisdictions, the Regulations allow parties to close their transaction at any time once they have notified the CCC.

According to the new Guidelines, the CCC will complete its Phase 1 investigation within 45 calendar days of receiving a complete filing. If the CCC decides to open a more detailed Phase 2 investigation, it will issue its final decision within 120 days of the initial filing date. Both phases may be subject to extensions that cumulatively do not exceed 30 days. Further, if the CCC requests additional information from a party, it may suspend Phase 2 for some amount of time to allow for the receipt of the additional information.

> "The thresholds for notification are quite low in comparison with other jurisdictions."

For transactions that may exceed these thresholds, but which the parties do not believe would have an appreciable effect on trade between Members States or restrict competition in the Common Market, the acquiring person (either alone or jointly with other parties to the merger) may request a "comfort letter" from the CCC advising that the transaction is not notifiable. As with the merger notification, the request for a comfort letter must be received no later than 30 days after the decision to merge. Within 21 days of a request for a comfort letter, the CCC will provide the letter and a request for additional information or documents or inform the parties that a merger notification is required.

Filing Fee

The Guidelines did not address the filing fee. Under the Regulations, the parties must pay a filing fee of the lower of either

- 0.5 per cent of the combined annual turnover or the combined value of the assets of the merging parties in the Common Market, whichever is higher
- US$500,000

This is quite high in comparison with other jurisdictions. The European Union does not have a filing fee, and the largest filing fee in the United States (based on the size of the transaction) is US$280,000.

Referrals

Although the Regulations are meant to provide a sort of one-stop shop for merger review within the Common Market, a Member State may request that the CCC refer the merger to its national competition authority. The Guidelines outline the timing and procedures for referrals. No additional filing fee will be required in the event the merger is referred to a Member State.

Amnesty

Failure to notify a transaction may incur fines of up to 10 per cent of the parties' combined turnover in the Common Market. For parties that implemented mergers prior to 31 October 2014 that were not, but should have been, notified, the CCC will not impose penalties for the failure to file, provided the merger is notified to the CCC by 29 January 2015.

Practical Implications

Companies engaged in international mergers and acquisitions must consider the potential for filing obligations in COMESA in connection with multijurisdictional transactions.

Although the CCC has clarified when a transaction may be reportable, the thresholds for notification are quite low in comparison with other jurisdictions and should therefore be checked carefully.

Although the CCC has not imposed any fines to date, the Guidelines' amnesty provision suggests that the CCC may be more inclined to impose penalties for failures to file now that it has provided clearer thresholds. Further, while the Regulations do not have a suspension requirement, closing in advance of the CCC's decision carries the risk that the CCC may find the merger unlawful and require some remedial action, including dissolution of the merger.

Until the CCC develops more of a track record in analysing mergers, it will be difficult to assess the risk of closing certain mergers prior to the CCC's decision. Transactions involving businesses operating in the COMESA region, which comprises much of southern and eastern Africa, should be assessed in every case to determine whether or not obligations arise under COMESA.

Carla Hine is a partner based in the Firm's Washington, DC, office. She focuses her practice on antitrust and consumer protection regulatory matters. She defends mergers and acquisitions before the US antitrust agencies and international competition authorities, and has experience with administrative Part III litigation before the Federal Trade Commission. Her antitrust practice includes counselling, government investigations and antitrust litigation. Carla can be contacted on **+1 202 756 8095** or at **chine@mwe.com**.

Conversion to a German Company: An Option for EU Businesses

By **Clemens Just** and **Kian Tauser**

Cross-border transfers of companies into or out of Germany have, up until now, been achieved as a cross-border merger. Case law now provides another option: companies may move from an EU Member State to Germany, or from Germany to another EU Member State, by means of a cross-border conversion *(grenzüberschreitender Formwechsel)*.

Cross-border conversions involve a straightforward transfer of the corporate seat, which is a more flexible and cost-efficient option than a cross-border merger. The key aspect of a conversion is the maintenance of the company's legal identity. Contracts and property rights continue and it is not necessary to transfer any contracts or assets.

A cross-border conversion might be necessary in the course of an international restructuring, a post-acquisition integration or after a change of market conditions. In most cases, change of control clauses are not triggered and permits for operation will usually also continue.

The Higher Regional Court of Nuremberg has become the first German High Court to allow an inbound cross-border conversion of a non-German corporation into a German limited liability company (GmbH). In theory, an outbound transfer of a German company to another EU Member State should also now be possible.

Legal Landscape

The Higher Regional Court of Nuremberg's decision (Case No. 12 W 520/13) dealt with a conversion of a private limited liability company organised under the laws of Luxembourg (*Société anonyme à responsabilité limitée* (S.à r.l)) into a private limited liability company under German law.

The company applied for registration with the German commercial register, and for conversion into a German limited liability company. Upon application, the company was deregistered from Luxembourg but the registration was rejected by the German regional court. This decision was overruled by the High Court of Nuremberg, which based its decision on the judgment of the Court of Justice of the European Union (CJEU) in *VALE* 12 July 2012 Case No. C-378/10, which provided for authorisation of cross-border conversions.

Even though the *VALE* judgment was handed down in 2012, the precise procedural rules, in particular how local commercial registers would apply the CJEU's ruling, remained unclear until the Nuremberg decision.

Under European law, the freedom of establishment demands that a cross-border conversion must take place under the same conditions as a conversion of a domestic company. The German Transformation Act only allows a conversion for legal entities that have their registered office in Germany. The Higher Regional Court of Nuremberg acknowledged that the German Transformation Act has to be interpreted under European law, and that aspects of the act that may form a barrier to cross-border conversions will be changed.

Tax Aspects

A cross-border conversion of a company affects certain aspects of income tax, *e.g.*, tax losses, interest carry-forwards and exit tax, plus real estate transfer tax.

Inbound Conversion

The inbound conversion of a foreign company to be registered in Germany does not have detrimental effects on existing tax losses or the interest carry-forward that is recognised for an existing permanent establishment. By converting to having a permanent German base, a foreign company, *e.g.*, a UK Ltd converting its headquarters to Germany, is subject to limited taxation on inbound income.

German tax losses applicable to a permanent German headquarters of a foreign company remain unaffected by an inbound conversion. This is because the company's shareholders, as well as its legal identity, remain in place despite the cross-border conversion.

With an inbound conversion, *e.g.*, the change of a UK Ltd to a German GmbH, the company becomes subject to unlimited German tax liability. A cross-border conversion of a foreign company to Germany may have negative effects on the company's international tax liabilities, *e.g.*, exit tax, forfeiture of tax losses and interest carry-forward. This should be considered in the tax planning.

Outbound Conversion

Tax planning for outbound conversions should particularly consider the conversion's effect on existing tax losses, interest carry-forwards and potential exit tax.

If, as a result of the outbound conversion, no German permanent establishment remains, existing tax losses and interest carry-forwards cease to exist. Further, should Germany lose its right to tax assets, an exit tax is triggered on related hidden reserves.

This applies to the extent that the company's assets do not remain in Germany, but move abroad with the company. Only the country of destination has the right of taxation, in accordance with relevant double tax treaties.

German tax law allows for the tax effect to be applied over five years, rather than immediately.

If the outbound conversion is of an empty German holding company, this has to be structured with caution in order not to create taxable restructuring-related profit as a result.

Real Estate Transfer Tax

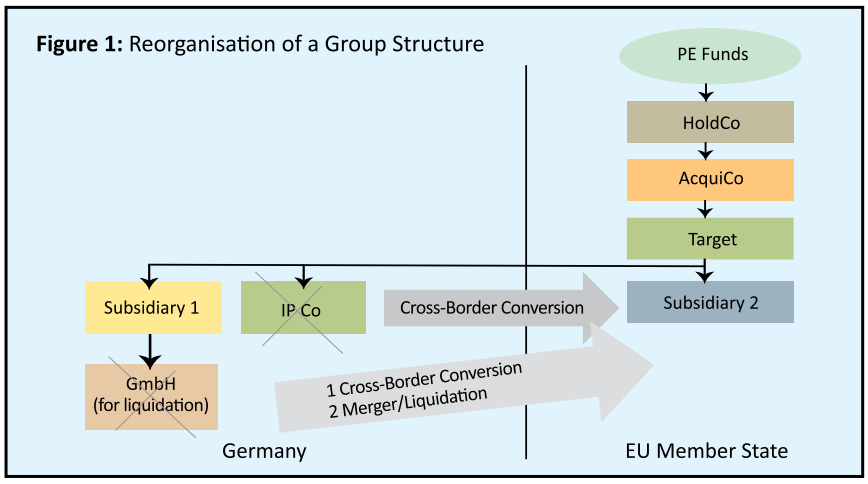
Because the legal identity of the company remains unchanged, from a German real estate transfer tax (RETT) perspective, transfers of real property or alterations to the shareholding of the company are not necessary. As a consequence, cross-border conversions do not trigger RETT, which makes them a RETT-efficient reorganisation measure.

Practical Examples

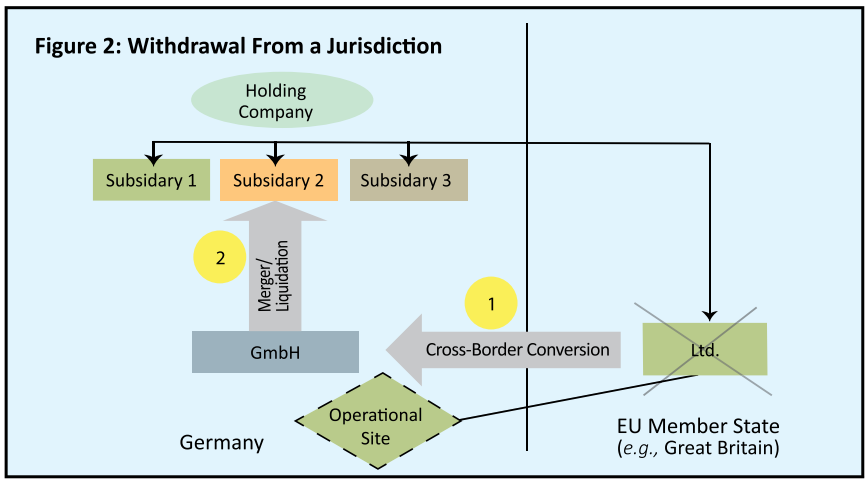
A cross-border conversion can also be a method for simplifying or specifically tailoring group structures, or a simple way to liquidate a company. Examples include

- **Reorganisation of a group structure** (see Figure 1): After an acquisition or, in the course of a restructuring, a service company is relocated to another EU Member State. For example, a German IP or service centre company is transferred to the Netherlands.
- **Withdrawal from a jurisdiction** (see Figure 2): The company's business is focused on the market of another Member State. By converting its seat to that State, the high administrative costs of a foreign legal form, *e.g.*, annual financial statements and tax returns, can be avoided in the future. For example a UK Ltd is practically only operative in Germany, so it transfers its seat to Germany.
- **Tax-neutral optimisation of real estate companies** (see Figure 3): A real estate holding company is organised as a German limited partnership (KG). Ancillary services provided by the KG to its tenants result in the KG being subject to trade tax. As a matter of precaution, the seat of the KG is transferred to Luxembourg, changing the form into a Luxembourg limited partnership. As the legal identity of the partnership does not change, no RETT is triggered.
- **Fast-track liquidation**: Functionless companies, *e.g.*, empty holdings after an exit, can be liquidated without much effort in a Member State that offers a flexible legal framework. For example, a GmbH can only be liquidated after a one-year blocking period. It is therefore an option to transfer the company to another EU Member State that has a more flexible company liquidation regime.

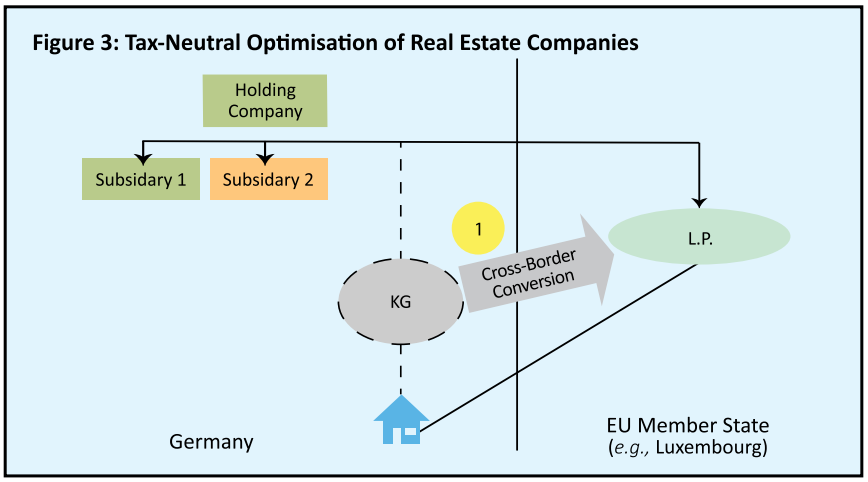
Cross-Border Conversion in the European Union



Cross-Border Conversion to Germany



Cross-Border Conversion to Luxembourg



Clemens Just is a partner based in the Firm's Frankfurt office. He advises on all aspects of corporate law and M&A transactions and on private and public takeovers. His experience includes corporate restructurings and insolvency law issues. Clemens can be contacted on **+49 69 951 145 123** or at **cjust@mwe.com**.

Kian Tauser is a partner based in the Firm's Frankfurt and Munich offices. He advises clients on tax audits and the tax aspects of M&A transactions for strategic investors and private equity houses, reorganisations, restructurings, structured finance and fund structuring. Kian can be contacted on **+49 69 951 145 215** or at **ktauser@mwe.com**.

Are No Hiring and No Poaching Agreements Enforceable in Germany?

By **Volker Teigelkötter** and **Bettina Holzberger**

No poaching agreements between leading companies in the IT sector have recently caused a substantial scandal in Silicon Valley, California, resulting in tech industry businesses settling a major lawsuit by paying a reported US$324 million. Such agreements can be found all over the world; but are they enforceable in Germany?

Two Types of Agreements

It is important to differentiate between a no poaching agreement and a no hiring agreement. A no poaching (or no solicitation) agreement allows Company A to hire an employee of Company B, as long as Company A did not solicit, induce or entice that employee from Company B.

A no hiring agreement means Company A is prohibited from hiring an employee from Company B, even if the employee was neither solicited, induced nor approached in any other way by Company A, but applied for an advertised job on his or her own initiative.

No hiring agreements impact directly on the employee's independent ability to change employers. They also implicitly keep all salaries in the relevant industry and regional market at a certain level, as the companies in that industry and market do not compete to hire employees by offering them higher salaries. These companies are therefore able to keep salaries at their current level, and the employees have no leverage to ask their existing employer for an increase.

Are Either Type Enforceable in Germany?

In highly specialised industries in Germany, such as the IT sector, no solicitation and no hiring agreements between competitors do exist. These agreements can also be found in merger and acquisition transactions, where it is customary to agree on a list of employees who cannot be enticed away from the seller by the purchaser and vice versa.

Section 75f of the German Commercial Code expressly states that no hiring agreements are not enforceable. Even if companies have agreed in writing that they are mutually prohibited from hiring employees who work for the other party, that agreement cannot be enforced before a court. This is to protect the employees' constitutional right to freely choose a work place, which would otherwise be severely infringed by such an agreement.

> The German Commercial Code expressly states that no hiring agreements are not enforceable.

A decision by the Highest German Civil Court (the Bundesgerichtshof) dated 30 April 2014 has provided some clarity on no solicitation agreements. The court held that, generally, no solicitation agreements between companies are, just like no hiring agreements, subject to Section 75f of the German Commercial Code and, as such, are unenforceable. The ability of the employee to progress in his or her professional life, and to choose a workplace and employer freely, are infringed by a no solicitation agreement, as the employee is prevented from learning another company's interest in his or her professional abilities and therefore loses the opportunity to accurately gauge his or her commercial value and the option to change jobs.

The Bundesgerichtshof also, however, provided for exceptions. Most importantly, if the companies have a trusted relationship, and the no solicitation agreement is intended to improve loyal cooperation, a no solicitation agreement might be legal and enforceable. The agreement may, however, only last for the active duration of this trusted relationship and for up to a maximum of two years thereafter.

Third Party Rights

If an employee can prove that a no solicitation or no hiring agreement was in place, and he or she suffered specific damage as a result, *i.e.*, received a salary lower than he or she would have received if the agreement hadn't been in place, it might be possible to enforce a claim and the employee could be reimbursed for the specific financial damage suffered.

Volker Teigelkötter is a partner based in the Firm's Düsseldorf office. He heads the German Labour and Employment Group, where his practice covers the entire spectrum of labour and employment law. Volker can be contacted on **+49 211 30211 311** or at **vteigelkoetter@mwe.com**.

Bettina Holzberger is an associate based in the Firm's Düsseldorf office. She advises on all individual and collective aspects of labour and employment law. Bettina can be contacted on **+49 211 30211 313** or at **bholzberger@mwe.com**.

Learn More

Stay up to date with current legal issues and industry trends through McDermott's other publications, blogs and tweets.

Our publications are all accessible from www.mwe.com and include

- *China Law Alerts*
- *Focus on China Compliance*
- *Focus on Private Equity*
- *Focus on Regulatory Law*
- *Focus on Tax Controversy*
- *Focus on Tax Strategies & Developments*
- *Inside M&A*
- *IP Update*
- *On the Subjects*
- *Special Reports*
- *UK Employment Alerts*

Sign up at www.mwe.com/subscribe/to receive regular updates direct to your inbox.

Stay connected on business issues and visit McDermott's blogs:

www.alcohollawadvisor.com
www.antitrustalert.com
www.corporatedealsource.com
www.employeebenefitsblog.com
www.energybusinesslaw.com
www.healthcarelawreform.com
www.insidesalt.com
www.mwe-blogar.de
www.ofdigitalinterest.com
www.transferpricing360.com

Follow us on Twitter @McDermottLaw

Our *On the Subjects* provide insight into key legal developments and the way in which those developments affect business. A recent selection includes the following:

- ISS and Glass Lewis Update Proxy Voting Guidelines for 2015
- "Gun-Jumping" Companies Must Pay $3.8 Million in Fines and Disgorge $1.15 Million in Illegally Obtained Profits
- CMS Finalizes Proposal to Remove Continuing Medical Education Exclusion from Sunshine Act Regulations
- Holiday Pay - Not As Bad As It Could Have Been
- Italian Competition Authority Issues Guidelines on Antitrust Infringement Fines
- Restrictive Covenants: An Important Reminder for Employers

McDermott
Will & Emery

www.mwe.com/international/

BOSTON
28 State Street
Boston, MA 02109
USA
Tel: +1 617 535 4000
Fax: +1 617 535 3800

BRUSSELS
Avenue des Nerviens 9 - 31
1040 Brussels
Belgium
Tel: +32 2 230 50 59
Fax: +32 2 230 57 13

CHICAGO
227 West Monroe Street
Chicago, IL 60606
USA
Tel: +1 312 372 2000
Fax: +1 312 984 7700

DÜSSELDORF
Stadttor 1
40219 Düsseldorf
Germany
Tel: +49 211 30211 0
Fax: +49 211 30211 555

FRANKFURT
Feldbergstraße 35
60323 Frankfurt a. M.
Germany
T: +49 69 951145 0
F: + 49 69 271599 633

HOUSTON
1000 Louisiana Street
Suite 3900
Houston, TX 77002
USA
Tel: +1 713 653 1700
Fax: +1 713 739 7592

LONDON
Heron Tower
110 Bishopsgate
London EC2N 4AY
United Kingdom
Tel: +44 20 7577 6900
Fax: +44 20 7577 6950

LOS ANGELES
2049 Century Park East
38th Floor
Los Angeles, CA 90067
USA
Tel: +1 310 277 4110
Fax: +1 310 277 4730

MIAMI
333 Avenue of the Americas
Suite 4500
Miami, FL 33131
USA
Tel: +1 305 358 3500
Fax: +1 305 347 6500

MILAN
Via dei Bossi, 4/6
20121 Milan
Italy
Tel: +39 02 78627300
Fax: +39 02 78627333

MUNICH
Nymphenburger Str. 3
80335 Munich
Germany
Tel: +49 89 12712 0
Fax: +49 89 12712 111

NEW YORK
340 Madison Avenue
New York, NY 10173
USA
Tel: +1 212 547 5400
Fax: +1 212 547 5444

ORANGE COUNTY
4 Park Plaza
Suite 1700
Irvine, CA 92614
USA
Tel: +1 949 851 0633
Fax: +1 949 851 9348

PARIS
23 rue de l'Université
75007 Paris
France
Tel: +33 1 81 69 15 00
Fax: +33 1 81 69 15 15

ROME
Via A. Ristori, 38
00197 Rome
Italy
Tel: +39 06 462024 1
Fax: +39 06 48906285

SEOUL
18F West Tower
Mirae Asset Center1
26, Eulji-ro 5-gil, Jung-gu
Seoul 100-210
Korea
T: +82 2 6030 3600
F: +82 2 6322 9886

SHANGHAI
MWE China Law Offices
Strategic alliance with
McDermott Will & Emery
28th Floor Jin Mao Building
88 Century Boulevard
Shanghai Pudong New Area
P.R. China 200121
Tel: +86 21 6105 0500
Fax: +86 21 6105 0501

SILICON VALLEY
275 Middlefield Road
Suite 100
Menlo Park, CA 94025
USA
Tel: +1 650 815 7400
Fax: +1 650 815 7401

WASHINGTON, D.C.
The McDermott Building
500 North Capitol Street, N.W.
Washington, D.C. 20001
USA
Tel: +1 202 756 8000
Fax: +1 202 756 8087

McDermott's international legal professionals advise multinational entities on cross-border legal matters. Interdisciplinary practice groups, integrated by practice rather than geography, allow our lawyers to respond to challenges our clients face, day or night.