Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

Business ethics and anti-corruption world

A global bulletin on recent business ethics and anti-corruption developments

Issue 05 / February 2017

In this issue:

Foreword

Welcome to the fifth edition of Business ethics and anti-corruption world. As with our previous issues, we aim to highlight Norton Rose Fulbright's global reach through analysis and reflection of key updates and events related to business ethics, anti-corruption and business and human rights developments.

Our business ethics and anti-corruption practice helps clients to navigate national and international anti-corruption, regulatory and compliance issues and investigations wherever they arise. We advise corporates, financial institutions and senior executives extensively on the implications of international business ethics and anti-corruption best practice standards, wider developments in the legislative and corporate landscape, and in relation to internal and government-led investigations. We work closely with colleagues across our global platform of more than 50 offices throughout Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia to advise clients on international compliance needs across a wide range of risks.

Our team also recognizes that human rights represent an evolving area of emerging risk for businesses which is assuming an increasingly legal dimension. With initiatives like our recently published joint Business and Human Rights Due Diligence Project with the British Institute of International and Comparative Law (see article below), we are a leading force in providing guidance to businesses on human rights related risks and obligations.

In this edition we

- Highlight the proposed amendment to the Criminal Finance Bill, which reflects a broader agenda which aims to ensure that financial institutions and other professional service providers do not facilitate the retention of funds derived from human rights abuses.
- Reflect on the publication of the ISO standard for anti-bribery management systems and how to test if anti-bribery management programmes truly are effective.
- Comment on the remediation standards for FCPA compliance programmes.
- Summarize the recent Nu Skin settlement with the FCPA.
- Discuss how Singaporean authorities are using a prosecutorial techniques similar to US-style 'books and records' offences to bring senior managers to account for corrupt schemes.
- Summarize and comment on the World Bank's suspension and debarment system.
- Highlight the UK's second deferred prosecution agreement (XYZ Limited) and note similarities between this case and the UK's first deferred prosecution agreement (Standard Bank).
- Comment on the legal issues raised by engagement, monitoring and termination of third parties.
- Highlight the need for testing and assurance of ethics and compliance programme.
- Interview a senior counsel of an international provider of testing, inspection and certification services on compliance due diligence.
- Provide an overview of new trends and developments in connection with compliance due diligence processes in Germany.
- Highlight a recent legal precedent related to bribery and public policy in the English courts.
- Provide an overview of key findings from our recently published joint project with the British Institute of International and Comparative Law on human rights due diligence.

If you would like to discuss business ethics and anti-corruption issues relevant to your organization, please feel free to contact us or our global network. Contact details are at the end of this issue.

More than 50 locations, including Houston, New York, London, Toronto, Hong Kong, Singapore, Sydney, Johannesburg, Dubai.

Attorney advertising

Contents

Human rights and finance: an angle for NGOs

An amendment to the Criminal Finances Bill[1] (the Bill) currently before Parliament has recently been proposed to amend the Proceeds of Crime Act 2002 (POCA) to allow the High Court to make orders designating the conduct of a person – wherever it occurs – as connected to a gross human rights abuse, and to set prohibitions on that person's ability to deal with property, funds and finances and access related services. Following an order designating conduct as connected to a gross human rights abuse it will be incumbent on the relevant authorities to seek a civil recovery order of any proceeds of such conduct.

The amendment has cross-party support and, all things being equal, stands a good chance of being adopted. It anticipates an important role for civil society by empowering individuals and NGOs to make applications for designating orders. This bears some resemblance to the proposed Global Magnitsky Human Rights Accountability Act in the US, which would require the President to consider 'credible information' obtained by NGOs of human rights abuses when determining whether to apply sanctions on foreign individuals or entities. This potentially represents the beginning of a broader trend towards a greater reliance by governments on the expertise and evidence-gathering skills of NGOs to ensure effective enforcement action against persons responsible for human rights abuses.

The amendment also reflects a broader agenda which aims to ensure that financial institutions and other professional service providers do not facilitate the retention of funds derived from human rights abuses. Mindful of the reputational and legal risks associated with dealing in such assets, as well as the expectations of the *UN Guiding Principles on Business & Human Rights* (UN Guiding Principles), a growing number of financial institutions are reviewing their money-laundering policies and procedures as part of their human rights impact mitigation strategies.

The Amendment

Designating orders

The amendment proposes that the High Court be given the power to make an order designating that the actions of a person (the respondent) constitute conduct connected to a gross human rights abuse and further order that

- A person is prohibited from dealing with property, funds or economic resources owned, held or controlled by the respondent if the person knows or has reasonable cause to suspect that he/she is dealing with property, funds or economic resources owned.
- A person is prohibited from making property, funds or financial services available, directly or indirectly to the respondent if the person knows or has reasonable cause to suspect that he/she is making property, funds or economic resources services so available.
- A person is prohibited from making funds or financial services available to any person for the benefit of the respondent if the person knows or has reasonable cause to suspect that he/she is making funds or economic resources services so available.

1 The Criminal Finances Bill had its first reading on October 13, 2016. A Home Office press release of the same day stated that the bill was "new legislation to tackle money laundering and corruption, recover the proceeds of crime and counter terrorist financing".

These prohibitions will in effect prevent the respondent from dealing with his assets or availing himself of services in relation to his property, funds or finances. They can be imposed for a maximum of two years, and there is no need to establish a connection between the gross human rights abuse and the property subject to the designating order.

An application for such an order may be made by the Government, individuals and entities, expressly including NGOs. The High Court must be satisfied that it is in the public interest to make such an order. The Government will be under a duty to apply for such an order where the requirements are met and it is in the public interest.

Conduct connected to a gross human rights abuse

Conduct connected to a gross human rights abuse is defined as

- Involvement by Person A in torture or other serious breaches of human rights and fundamental freedoms against Person B, where Person B sought or seeks to expose illegal activity carried out by foreign public officials or to obtain, exercise, defend or promote human rights and fundamental freedoms.
- Activities by Person C as an agent in connection with the activity by Person A.
- Activities by Person D to profit from, materially assist, sponsor or provide financial, material or technological support for, or goods and services in support of, the activity by Person A.
- Commission by Person E, whether or not a public official, of the illegal activity carried out by foreign public officials.

Civil recovery: gross abuse of human rights

Conduct that has been designated as connected to a gross human rights abuse and would amount to a criminal offence had it occurred in the UK will also be deemed to amount to what is known as ‘unlawful conduct’. This means that the proceeds of such conduct can be subject to the existing civil recovery regime under POCA. The relevant authorities will be under a duty to seek to initiate recovery proceedings where they have evidence of the existence of proceeds of conduct designated as connected to a gross human rights abuse.

Discussion

To date, the UK Government's efforts to curtail access to finance and financial services for human rights abusers has largely focussed on slavery and human trafficking. In particular

- The Modern Slavery Act 2015 (MSA) amended the list of 'lifestyle offences' in Schedule 2 of POCA to include offences under the MSA, making it easier for the prosecuting authorities to bring confiscation proceedings against persons convicted of slavery or human trafficking.

- The *Transparency in Supply Chains* etc. practical guide, published by the government to assist businesses in preparing slavery and human trafficking statements pursuant to section 54 of the MSA notes the risk of financial institutions laundering funds derived from modern slavery.

This amendment recognizes that abuses relating to a wider range of human rights can bring commercial benefits for perpetrators and their associates, and seeks to remove that financial incentive. Having said that, there remain a number of unanswered questions which the Court would need to consider if the amendment to the Bill became law in its current form.

Firstly, the amendment envisages that the respondent's abusive conduct would need to occur in response to another person seeking to 'exercise' human rights. It is unclear what circumstances would be necessary to fulfil this criteria. This may well be a low hurdle, as the Bill is already restricted to gross abuses.

The meaning of 'gross human rights abuse' has been the subject of much debate over the years. In a 1993 working paper, the UN Commission on Human Rights' Sub-Commission on Prevention of Discrimination and Protection of Minorities noted that "distinguishing between gross and less serious human rights violations ... cannot be done with complete precision". This reflects current thinking, although the following helpful guidance can be found in the Interpretative Guide to the UN Guiding Principles published by the Office of the United Nations High Commissioner for Human Rights (OHCHR).

There is no uniform definition of gross human rights violations in international law, but the following practices would generally be included: genocide, slavery and slavery-like practices, summary or arbitrary executions, torture, enforced disappearances, arbitrary and prolonged detention, and systematic discrimination. Other kinds of human rights violations, including of economic, social and cultural rights, can also count as gross violations if they are grave and systematic, for example violations taking place on a large scale or targeted at particular population groups.[1]

Ultimately, the effectiveness of the new law will hinge largely on the number of applications made to the High Court by NGOs capable of complex investigations involving asset-tracing exercises such as Global Witness, Amnesty International and Human Rights Watch.

Such investigations are on the increase, and the link between human rights and finance is very much in focus. Against this backdrop, the amendment highlights the importance of financial institutions and other professional service providers ensuring their due diligence and on-going monitoring processes are well-attuned to identifying clients and business partners with potential links to human rights abuses.

1 OHCHR, *The Corporate Responsibility to Respect Human Rights: An Interpretative Guide*, United Nations, 2012, available at http://www.ohchr.org/Documents/Publications/HR.PUB.12.2_En.pdfsee (Accessed: December 21, 2016).

For more information contact:

Sam Eastwood
Head of business ethics and anti-corruption
Partner, London
Tel +44 20 7444 2694
sam.eastwood@nortonrosefulbright.com

Stuart Neely
Associate, London
Tel +44 20 7444 3289
stuart.neely@nortonrosefulbright.com

But does it really work? The value of ISO certification of anti-bribery compliance

The highly-anticipated ISO standard for anti-bribery management systems – ISO 37001 – was recently published. The standard and its guidance represent the outcome of an arduous process, where stakeholders from many nations and representing a range of interests agreed a set of principles that organizations of all sizes (whether public, private or not-for-profit) can use to design anti-bribery management programs. The ISO does not intend or purport to create new ground, but rather consolidates existing guidance from regulators, intergovernmental organizations and NGOs.

Organizations might consider obtaining ISO certification for any range of reasons. First and foremost, such a certification can indicate to a company's customers, business partners, investors and any others exposed to the company's risk profile that the organization's program meets baseline standards.

However, companies considering certification should be mindful that an ISO 37001 certification means that an anti-bribery management program of a certain design exists, with all of the constituent parts prescribed by ISO; it does not mean that the program really works. This is an important point, as any government agency looking to take enforcement action against an organization for bribery and corruption related offences will inevitably undertake its own assessment of whether that organization's compliance program is genuinely effective in its day-to-day application.

ISO 37001 in summary

In terms of content, ISO 37001 defines bribery by reference to the laws applicable to each organization and prescribes various actions, measures and controls that would be familiar to experienced legal, compliance and risk professionals. These include

- Conducting a risk assessment to determine the risks faced by the organization.
- Providing related training for all relevant employees and business associates.
- Conducting appropriate due diligence to assess bribery risks.
- Top management leadership and commitment.
- Providing appropriate resources for the operation of the anti-bribery management system.
- Implementing appropriate financial and commercial controls to mitigate the risk of bribery.
- Having whistle-blowing procedures in place.
- Monitoring and testing the program's effectiveness on a regular basis.

ISO certification can be a useful indication to external stakeholders that these elements exist within an organization. For the business partner who requests information about a company's anti-bribery management program, ISO certification could be shorthand for describing the various elements in place.

Further, regulators who want to encourage a compliance culture in jurisdictions with less enforcement history than the United States or United Kingdom may point to ISO 37001 as guidance for local organizations. Because ISO 37001 is a global commercial standard, it may be better received than standards promulgated by the US or UK regulators, whose extraterritorial reach is sometimes perceived as unreasonable.

Genuinely effective?

Anti-bribery management programs have two main aims

- To mitigate the risk and incidence of corruption within an organization.
- To provide a credible response to prosecutors when, despite best efforts, a corrupt act occurs.

Programs that achieve those two aims are those that actually work, rather than just exist.

The message from relevant authorities is unambiguous: only truly effective anti-bribery management programs merit consideration in terms of penalty mitigation or, where applicable, an affirmative defence. In fact, the *UK Government Guidance on Corporate Prosecutions*[1] lists an ineffective compliance program as an aggravating factor that should encourage a decision to prosecute. Similar language appears in the *UK Deferred Prosecution Agreements Code of Practice*.[2] A key takeaway from the Standard Bank DPA is that ineffective anti-bribery programs will not be considered 'adequate procedures', despite the moving parts that may exist.[3]

US authorities ask three basic questions: "Is the company's compliance program well designed? Is it applied in good faith? Does it work?".[4] US regulators often give some weight to a respondent's compliance program, but mitigation is only awarded in cases where the program is truly effective – and where the alleged corrupt activity took place despite the company's best efforts.

What is a corporate to do?

ISO certification could certainly be a valuable exercise for any organization looking to ascertain whether its program – or at least its plan for developing the program – hits all

1 See page 7, available at: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/codes-and-protocols/.
2 See page 5, available at: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/deferred-prosecution-agreements/.
3 For further information about the Standard Bank DPA, please see Norton Rose Fulbright's prior client alert.

4 See page 56, available at: https://www.sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf.

the right marks. Seeking certification should not, however, direct company resources away from focussing on meeting the standards regulators set: is the program mitigating the risk and incidence of corruption, and is it providing a credible response when impropriety nonetheless occurs?

Achieving these goals – as opposed to a certification – is hard work and takes planning, expertise and cultural change management. Reflecting this, the ISO standard notes in its appendix that senior managers must have 'genuine intent' and a 'genuine commitment to prevent, detect and address bribery in relation to the organization's business'.[5] This matches various guidance documents issued by the authorities, such as the *UK Ministry of Justice Bribery Act Guidance*,[6] the *FCPA Resource Guide*[7] and the *US Federal Sentencing Guidelines*.[8]

The dangers of an over-reliance on certification were highlighted earlier this year when Australian journalists alleged that Monaco-based Unaoil had helped various multi-national companies secure government licences using improper payments. Unaoil had previously been certified by a well-known due diligence provider. The matter is now subject to a number of criminal inquiries by authorities including the SFO, and the press has labelled the agent, 'The intermediary that allegedly bribed the entire oil industry'.[9]

Ensuring that your anti-bribery management program really works takes genuine review and assurance: not just an auditing process, but substantive transaction testing to ensure that legal risks are being appropriately identified and mitigated, that processes are being followed and that the correct decisions are being made by businesses, legal and compliance personnel. Such an outcomes-based assessment provides metrics and management information to executives and boards, which enables a company to determine with confidence whether their program really works. The same can be done, albeit with more qualitative feedback, with respect to development of ethical culture and training effectiveness. What dilemmas are facing your managers, and how effectively does their reflex meet the challenge? Is your training program changing hearts and minds, and how can you do better? Is your message being heard?

Real commitment and action is the challenge in any organization and the key to effective anti-bribery management programs. The new ISO standard gives corporates a set of tools by which they can meet that challenge, but whether those tools are deployed effectively is a matter of real testing and assurance.

Norton Rose Fulbright was delighted to be represented as the only legal practice on the UK based BSi Anti-Bribery Committee which worked on the ISO standard on anti-bribery (ISO 37001). This followed our earlier work on the British Standards Institute's panel in connection with the drafting of the first British Standard on Anti-Bribery (BS 10500).

For more information contact:

Jason Hungerford
Partner, London
Tel +44 20 7444 2474
jason.hungerford@nortonrosefulbright.com

Stuart Neely
Associate, London
Tel +44 20 7444 3289
stuart.neely@nortonrosefulbright.com

Paul Sumilas
Senior associate, Singapore
Tel +65 6309 5442
paul.sumilas@nortonrosefulbright.com

5 See paragraph A.3.1., available at: http://www.iso.org/iso/catalogue_detail?csnumber=65034.
6 See in particular Principle 2, available at: https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf.
7 See page 56, available at: https://www.sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf.
8 See § 8B2.1(b), US Sentencing Guidelines, available at: http://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2014/CHAPTER_8.pdf.
9 http://www.forbes.com/sites/jwebb/2016/07/26/serious-fraud-office-moves-against-unaoil-the-intermediary-firm-that-bribed-the-entire-oil-industry/#6d8b5aad435c.

Culture and compliance – new best friends?

Following the release by the United States Department of Justice (DoJ) of new remediation standards for FCPA compliance programs (see: DOJ launches pilot program for FCPA cases), compliance professionals are once again revisiting the key components of their programs. Beyond the US, the standards reinforce the requirements of the Bribery Act in the UK[1] and prospective legislation in other jurisdictions which is seeking to place a similar onus on businesses to prevent, detect and report financial crime.

Key elements the DoJ will assess in determining effectiveness of a compliance program are

- The 'culture of compliance'.
- The resources dedicated to the compliance function.
- The quality of the compliance personnel.
- The independence of the compliance function.
- Whether the compliance program has performed an effective risk assessment.
- How compliance personnel are compensated and promoted.
- Auditing of the compliance program.
- The reporting structure of compliance personnel within the company.

The challenge for businesses is to go beyond a 'tick- box' approach to compliance, to implementing, and maintaining, a positive culture of compliance. The above criteria alone may prove challenging for businesses headquartered beyond the United States in jurisdictions where compliance and its associated concepts may be less developed. Below, we consider how organizations might steer their employees towards complying both with the letter of the law and, just as critically, the spirit of the law.

1 Note that the UK Ministry of Justice is now consulting on plans to extend the scope of the criminal offence of a corporate 'failing to prevent' beyond bribery and tax evasion to other economic crimes.

Establishing a culture of compliance

'Culture' in this context is not easily defined and will vary between businesses. An organization should have a clear sense of purpose, with every employee, wherever located or in whichever business line, knowing what the organization stands for. In large multi-nationals, this will be difficult. The more remote an office in terms of its geography, including distance from and degree of control by 'headquarters', the harder it can be to assert a particular global culture. As Hui Chen, DoJ Compliance Expert has acknowledged[1], compliance officers often have to 'help their colleagues … navigate towards [compliance] expectations in societies that are not necessarily accustomed to these behaviors'.

The establishment of a robust sense of purpose that can withstand the pressures of the local environment is not easy. A concise set of values, communicated both internally and externally, is a first step, providing a reference point for the standards according to which an organization wishes to conduct its business and by which it would like to be judged. Those

1 Interview with *Ethics & Compliance Initiative*, February 1, 2016.

values need to be reiterated at the start of every new policy, survey or training so that all rules and guidance are set out in context.

The recent Deferred Prosecution Agreement agreed between the UK's Serious Fraud Office (SFO) and Standard Bank Plc[2] reveals the extent to which the SFO, and indeed the courts, will test the underlying culture of compliance within an organization when considering a potential settlement; in this case, the compliance training was deemed to be inadequate and the internal policies not sufficiently well-understood. Combined with a lack of co-ordination between group entities, this resulted in the compliance procedures as a whole being found to be lacking taking into account the risks posed.

The senior management of a company, including the most senior executives, undoubtedly have the greatest influence in driving a particular culture. They need to lead by example and establish the appropriate 'tone from the top'. A compliance program that lacks the visible and demonstrable backing of senior management will have limited effect. Senior management should make ethical conduct and ethical decision-making normal business practice and emphasise, through their messaging and conduct, the importance of a compliant culture. To do so, they will need to be well-informed about each element of the compliance program, being provided with high-quality management information and updated risk assessments. That way, they can ensure that the program is embedded across the business when visiting different offices, communicating with country or divisional management, and generally on a day-to-day basis.

Regular communication by leadership, both internally and externally, about the company's values, compliance initiatives, and stakeholder response to any compliance progress made, will serve to promote effective compliance as a key business strategy. Thus, responsibility for 'compliance' should be shared across the company and compliance fully integrated with other risk management functions. The HR function, for example, should be aligned with compliance to conduct background checks, to test attitudes to compliance during recruitment and promotion, to assess the impact of remuneration practices and incentives on culture, to engage in relevant disciplinary action and to report on 'lessons learned'. As Hui Chen has stated[3], "compliance can identify issues in a company's financial controls, HR processes, or sales strategy but ... without the commitment of finance, HR or sales leadership, these issues cannot be remediated."

A framework of employee engagement, feedback and review is important to sustain the established culture. The results of this engagement should be subject to review and analysis which should in turn inform changes to the program. Following instances of unethical behavior, there should be demonstrable sanctions, which could include such things as claw-back of bonuses and demotion. Equally critical, appraisals should start rewarding behaviors that go toward embedding the company's values and move away from traditional metrics that often have a narrow focus on achieving financial targets.

Dedicating sufficient resources to the compliance function

Embedding a compliant culture takes more than 'tone from the top'. The most demonstrable evidence of a company's commitment to a compliant culture is the extent of the resources allocated to the compliance function.

Human resource and budget (with compliance having its own independent budget, rather than shared with, say, the office of the General Counsel) is key. These resources should be sufficient to allow effective integration across the business, proportionate to the size of the organization, and reflect the risk of doing business in the relevant sectors and jurisdictions. An effective compliance program cannot be static. A company should periodically review its compliance program and update in light of new developments, such as changes in business focus, new regulatory pronouncements or other developments pertinent to the company's operations. Ideally, resources should extend to the periodic engagement of external consultants to provide an independent analysis of the effectiveness of the compliance program and insight on how to build or sustain the desired culture.

Ms Chen argues[4] that, in all areas, "strong compliance must be data driven". Therefore, resources should also allow a compliance function to use technology to facilitate the assessment, limitation and detection of risk, taking into account the proliferation of ever-changing business systems.

2 *SFO v Standard Bank Plc*, November 30, 2015 – Case no: U20150854.

3 Interview with *Ethics & Compliance Initiative*, February 1, 2016.

4 *Ibid.*

A compliance function created as an after-thought out of necessity in, say, rushed remediation efforts will struggle to be effective. However, a function established to work in tandem with senior management, which is fully and thoughtfully resourced and integrated with other risk management functions, will play a significant role in an organization meeting its strategic compliance objectives.

Quality and experience of compliance personnel

The DoJ considers whether compliance personnel can understand and identify transactions identified as posing a potential risk. Compliance professionals should have relevant qualifications and experience for the role. Personal qualities are equally important; the head of compliance should be an individual of sufficient gravitas to reinforce the importance which management places on compliance and ethical conduct.

According to Hui Chen[5], being in compliance requires "backbone and good judgment and excellent people skills". With the right characteristics, a successful head of compliance can engage effectively to attract the support of the entire work-force. This support will underpin changes in compliance culture far more effectively than, say, a whistleblowing hotline or online training program.

Compliance personnel should be proactive in learning about the risks implicit in their organization's sector including continually anticipating new, emerging risks. They should learn from their peers through networking at industry events and sharing best practice. It is often instructive to learn from those operating in sectors with greater exposure to risk or more experience in establishing effective compliance.

Independence of the compliance function

The DoJ expects that compliance personnel and, in particular, the head of compliance, are not placed in a position of possible conflict of interest between their compliance work and other responsibilities. It is thus prudent for an organization, where possible, to require compliance personnel only to perform compliance tasks. If this is not realistic, such as in smaller companies, appropriate steps should be taken to ensure potential conflicts of interest are avoided.

The concept of independence does not rule out close co-operation between the compliance function, management and staff. This relationship will be crucial if compliance risks are to be detected early and managed effectively.

Whether the compliance program has performed an effective risk assessment and tailored the compliance program accordingly

The most effective compliance programs are underpinned by regular risk assessments. The concept of 'compliance by design', pursuant to which the compliance program is tailored according to the sector that the organization is operating in, its geographical spread, case studies based on issues faced by competitors and the organization's own historical issues, is the most effective basis.

A risk assessment cannot be a one-off exercise but should be carried out as regularly as practicable. Businesses should assess the risks to which they are subject, analyze the most significant risks and allocate sufficient resource to remediate accordingly.

Broader questions of culture, attitude and knowledge should be tested, measured and the information gleaned then used to enhance the program.

How a company's compliance personnel are compensated and promoted

If the commitment to a compliant culture truly exists, the management of regulatory risk will be afforded the same importance as that of other senior management positions. Consequently, businesses should assess carefully whether the pay and promotion prospects of its compliance personnel reflect this principle.

In a large organization, one would expect the remuneration of the head of compliance to be in line with other heads of department. To maintain independence, a sub-committee of the Board should determine the level of remuneration.

Any remuneration linked to the financial performance of the business line for which an individual exercises compliance responsibilities may undermine his/her independence and should be avoided. Remuneration related to the financial performance of the organization as a whole, however, is generally deemed to be acceptable. Promotion should be linked to the effective management of risk over a defined period, combined with noticeable improvements in culture.

5 *Ibid.*

Auditing of the compliance program to assure its effectiveness

The DoJ takes into account whether the compliance program has been the subject of an external or in-house audit, including whether it has been designed appropriately to identify key risks and, if so, what action has been taken. Any gaps noted should be remediated as soon as practicable and the program improved accordingly, not allowed to remain unchanged and stagnant until a particular event provides the necessary impetus for change.

In order to maintain a compliant culture, regular feedback (from both management and employees) on the compliance program, including levels of confidence in the ethical conduct of the leadership team, and monitoring to ensure continuous improvement, are crucial.

Reporting structure of compliance personnel within the company

The DoJ expects that the head of compliance should have formal reporting obligations directly to the board, or at the least the senior management team, to facilitate sufficient influence among leadership. Reporting too far down in a company structure may limit the effectiveness of a compliance leader.

The nature of the reporting line between the remainder of the compliance team and the head of compliance will depend on how the organization has chosen to organise its compliance function. Some companies opt for stand-alone compliance reporting lines; others report through the risk function; others report through the office of the General Counsel. However structured, organizations must have in place reporting lines that are clearly articulated and operationally effective.

Reporting outcomes (negative or positive) to management makes leaders accountable for compliance and allows them to assess how well the organization is managing its compliance risk.

There should be clear policies in place concerning the escalation of, and response to, significant issues. Direct access to the board should be granted to the head of compliance where necessary, such as in the case of possible breaches identified during the course of an investigation.

Conclusion

While there is no shortage of guidance concerning compliance 'best practice', the more intangible concept of 'culture' is more difficult to define.

At its most basic, culture should be the creation of a common purpose across an organization, with a set of values reinforced from the top that permeate through every aspect of the business. In contrast to a time when too many organizations' cultures were found by regulators and prosecutors to be failing, a compliant culture may start to become a company's most valuable asset. The challenge for businesses globally is to establish, maintain and resource an effective framework to support their desired culture of compliance.

For more information contact:

Sam Eastwood
Head of business ethics and anti-corruption
Partner, London
Tel +44 20 7444 2694
sam.eastwood@nortonrosefulbright.com

Kevin James Harnisch
Partner, Washington, DC
Tel +1 202 662 4520
kevin.harnisch@nortonrosefulbright.com

Holly Quinnen
Senior associate, London
Tel +44 20 7283 6000
holly.quinnen@nortonrosefulbright.com

SEC fines Nu Skin US$765,688 to settle FCPA charges

On September 20, 2016, Nu Skin Enterprises, Inc. (Nu Skin) paid US$765,688 to settle allegations by the US Securities and Exchange Commission (SEC) that Nu Skin violated the accounting provisions of the US Foreign Corrupt Practices Act (FCPA) in connection with a charitable donation.[1] Specifically, the conduct relates to payments made by Nu Skin's Chinese subsidiary, Nu Skin (China) Daily Use And Health Products Co. Ltd. (Nu Skin China) to a charity tied to a high ranking official in the Chinese Communist party.[2] Nu Skin China allegedly made the payment in an effort to end an investigation by the Chinese Administration for Industry and Commerce (AIC) into Nu Skin China's marketing and sales practices. The resolution underscores the importance of caution and diligence in making charitable donations in foreign countries.

Facts

The AIC had been investigating whether Nu Skin China had been conducting business activities in a particular city without the necessary licenses. In an effort to influence the AIC's investigation, a Nu Skin China employee contacted the Communist party official, who was also the former boss of the head of the AIC branch investigating Nu Skin China, and requested the name of a charity to which Nu Skin China could donate. The official suggested a charity that was created by an entity with which the official was previously associated.

After the discussion with the official, the AIC informed Nu Skin China that there was enough evidence to file charges that would result in a fine of RMB2.8 million (approximately US$431,088). Nu Skin China offered to "donate some money instead of [paying] a fine" to avoid any charges. Senior personnel at Nu Skin China also requested that the official personally intervene in the matter in exchange for a RMB1 million donation to the charity. Soon after the charitable donation was made, the AIC notified Nu Skin China of its decision to neither charge nor fine the company.

The parent corporation identified the donation as a potential FCPA issue before it occurred and recommended that its Chinese subsidiary consult with US counsel. US counsel recommended that the subsidiary include anti-corruption language in the donation agreement. The parent corporation reviewed the draft of the anti-corruption provisions, but they were removed by the subsidiary just prior to execution.

The SEC alleged that Nu Skin violated the FCPA's accounting requirements because it recorded the payment as a charitable donation and failed to adequately investigate the circumstances of the charity and donation.

1 SEC Charges Nu Skin Enterprises, Inc. with FCPA Violations, US Securities and Exchange Comm'n (September 20, 2016), https://www.sec.gov/litigation/admin/2016/34-78884-s.pdf.

2 Nu Skin Enterprises, Inc., Exchange Act Release No. 78884, at *2 (September 20, 2016).

Key takeaways

This settlement highlights a number of key issues for companies subject to the FCPA.

Charitable donations are back in the crosshairs

This is the second time that the SEC has brought an enforcement action based entirely on a charitable donation. Companies need to carefully scrutinize charitable donations in foreign countries to maintain compliance with the FCPA. They should always determine why the donation is being made and who outside the company requested it. Donations requested by foreign government officials should not be approved unless the company can prove it has no matters before the foreign government that the official may influence. The conclusions should be documented in advance of the donation.

Instilling a compliance culture

Multinational companies must not only embrace the 'tone at the top' message that US regulators identify as a key element of a compliance program, but also ensure that the proper tone permeates further down in the organization. This resolution demonstrates that the US regulators are not excusing US public companies when the parent corporation is asking the right questions. The parent corporation took appropriate action by requiring Nu Skin China to consult with external US counsel regarding the adequacy of the donation documentation. But the subsidiary ignored that advice and removed the anti-corruption terms from the donation agreement, without the knowledge of parent personnel. The regulators are holding US companies responsible for the unauthorized actions of subsidiary employees. US companies must follow up to make sure its anti-corruption instructions were followed.

Geographic risk

China continues to be a hot spot for corruption and a focus for the US regulators – in 2016 alone, the SEC has brought over ten actions based on misconduct in China. As this case shows, even companies taking appropriate steps, such as engaging external counsel to assist on corruption-related matters, must take special care in the region. In this regulatory environment, companies must consider whether to conduct anti-corruption audits and reviews of their Chinese operations.

For more information contact:

Wilson Ang
Partner, Singapore
Tel +65 6309 5392
wilson.ang@nortonrosefulbright.com

Michael Edney
Partner, Washington, DC
Tel +1 202 662 0410
michael.edney@nortonrosefulbright.com

Kevin James Harnisch
Partner, Washington, DC
Tel +1 202 662 4520
kevin.harnisch@nortonrosefulbright.com

Sun Hong
Head of Shanghai
Tel +86 21 6137 7020
hong.sun@nortonrosefulbright.com

Paul Sumilas
Senior associate, Singapore
Tel +65 6309 5442
paul.sumilas@nortonrosefulbright.com

Ilana B Sinkin
Associate, Washington, DC
Tel +1 202 662 4651
ilana.sinkin@nortonrosefulbright.com

This time it's personal: senior management liability in 'books and records' offences

Senior managers who choose to turn a blind eye towards the corrupt practices of their companies and the employees they supervise may find themselves personally liable for allowing the company's books to be altered to conceal the corrupt nature of the payments made – even if it could not be shown that they had actually engaged in the payment of bribes.

Corruption is by nature a secretive economic crime that is both difficult to detect and prove. As both the bribe giver and recipient are liable for the offence of bribery, there is little incentive for any party to a corrupt transaction to report the offence to the authorities or to fully cooperate in any investigation. Conversely, the parties may be more inclined to collude and conceal their involvement in the corrupt transaction. The difficulty in detecting and proving corruption is further complicated where a corporate entity is involved. In such cases involving the corporatization of bribery, complex corporate structures and creative accounting practices may be employed to conceal the involvement of the individuals, especially those occupying senior positions in the company.

Nevertheless, recent cases in Singapore have shown that Singapore authorities are prepared to deploy a range of prosecutorial techniques so as to bring senior managers to account for their role in corrupt schemes through false accounting and money-laundering offences. This approach shows a striking similarity with the US-style 'books and records' offences often used by US prosecutors in complex bribery schemes, and the new false accounting offences recently enacted in Australia which will bolster the anti-bribery toolbox of the Australian Federal Police, available at http://www.nortonrosefulbright.com/knowledge/publications/137893/new-false-accounting-offences-bolsters-bribery-toolbox-for-australian-federal-police.

ST Marine

In *PP v Han Yew Kwang*, Han Yew Kwang (Han), a former deputy president at ST Marine, was prosecuted for conspiring with a number of colleagues, who were all senior executives at ST Marine at the material time, to pay bribes to employees of ST Marine's customers in order to obtain business from these customers. An integral part of this scheme involved disguising the bribes as bogus entertainment expenses which were paid out from petty cash vouchers as approved by the senior management of ST Marine, i.e. the accused and his co-conspirators. It is pertinent to note that Han and his colleagues were not the ones who carried out the payment of the bribes. Rather, they approved the fraudulent petty cash vouchers, which they knew were not genuine entertainment expense claims, that were presented to them.

Even though Han and a number of his co-accused admitted their involvement and cooperated in the course of investigations, it was evident that proving the individual acts of bribery was difficult. This was because investigations were hampered by the fact that key witnesses and the receivers of the bribes were mainly located overseas.

Nevertheless, this difficulty was surmounted by the use of section 477A of the Penal Code Cap. 224 (section 477A), which criminalizes the falsification of a company's accounts by a clerk or servant of the company with intent to defraud. Given that the bribes were essentially paid out of petty cash payment vouchers falsely recorded as 'entertainment expenses', this approach had the effect of bringing the accused and his conspirators to account for their role in the corrupt scheme, i.e. for approving the individual fraudulent payments, in addition to the general conspiracy to pay bribes.

Questzone

The authorities adopted a similar tactic in the prosecution of Thomas Philip Doerhman (Doerhman) and Lim Ai Wah (Lim), who were sentenced to 60 and 70 months jail respectively on September 1, 2016, for falsifying accounts under section 477A and money laundering offences under the Corruption, Drug Trafficking and other Serious Crimes (Confiscation of Benefits) Act Cap. 65A (CDSA). Doerhman and Lim, who were both directors of Questzone Offshore Pte Ltd (Questzone), were prosecuted for conspiring with a third individual, Li Weiming (Li), in 2010 to issue a Questzone invoice to a Chinese telecommunications company seeking payment of US$3.6 million for a fictitious sub-contract on a government project in a country in the Asia-Pacific. Li was the chief representative for the Chinese company in that country. A portion of the monies paid out by the Chinese company to Questzone pursuant to its invoice was then subsequently redistributed by Doerhman and Lim to Li and the then Prime Minister of that Asia-Pacific country in 2010.

Even though no corruption charges were brought under the Singapore Prevention of Corruption Act against the parties, it is plainly conceivable that Questzone functioned as a corporate conduit for corrupt payments to be made. On the facts, some key witnesses were overseas – with Li having absconded soon after proceedings against him commenced. The use of section 477A and money-laundering charges under the CDSA allowed the prosecution to proceed against Doerhman and Lim as they only needed to prove that the invoice was false, in respect of the section 477A charge; and that the monies paid out pursuant to the invoice – which would be proceeds of crime or property used in connection with criminal conduct – were transferred to Li and the then Prime Minister of the Asia-Pacific country, in respect of the money-laundering offences.

US and Australian approach: 'books and records'

The use of false accounting offences to prosecute senior management for their involvement in corrupt transactions is well established in the US. The Securities and Exchange Commission (SEC) is known to utilise the 'books and records provision in the Foreign Corrupt Practices Act (FCPA) to prosecute senior managers in listed entities for their role in the corrupt transactions. The relevant provision requires listed entities in the US to keep books and records that fairly and accurately reflect the transactions of the corporation. Therefore, a scheme involving the doctoring or manipulating of company records in order to conceal the corrupt transactions would cause the company to be in violation of this provision. Senior management who engage in or otherwise permit such conduct could be found similarly liable.

As far back as 2009, the SEC has used the books and records provisions aggressively to charge individuals. In the Nature's Sunshine case, the CEO and CFO of the company were charged with FCPA violations for failure to adequately supervise employees to make and keep accurate books and records and implement an adequate set of internal controls, despite not having direct knowledge or involvement in the bribery scheme. In a more recent example, the SEC charged Ignacio Cueto Plaza (Cueto), the former CEO of LAN Airlines S.A. (LAN), for his role in authorizing US$1.15 million in payments to a consultant pursuant to a sham consulting contract. The SEC alleged that Cueto "understood that it was possible the consultant would pass some portion of the [payment] to union officials" in an effort to resolve a dispute between LAN and its employees. Although unable to prove that a bribe payment occurred, the SEC stated:

"The payments were made pursuant to an unsigned consulting agreement that purported to provide services that Cueto understood would not occur. Cueto authorized subordinates to make the payments that were improperly booked in the Company's books and records, which circumvented LAN's internal accounting controls."

In another recent example, the SEC charged Jun Ping Zhang (Zhang), the former CEO and Chairman of Harris Corporation's (Harris) Chinese subsidiary CareFx China, for his role in facilitating a bribery scheme that provided illegal gifts to Chinese officials in exchange for business. Pursuant to the scheme, Zhang authorized and approved false expense claims that were used to provide gifts to officials. The SEC charged Zhang with violations of both the anti-bribery and accounting provisions of the FCPA, alleging:

"[Zhang] was Harris' gatekeeper at CareFx China, but he nonetheless authorized false expense claims that he knew were going to be used to provide gifts to government officials. Moreover, Ping helped his subordinates at CareFx China hide the bribe scheme from Harris auditors and employees."

In a move that will bring the Australian anti-corruption regime closer to the US and Singapore approach, new offences involving false dealing with accounting documents came into effect on March 1, 2016. Under the new law, it is an offence for an individual or corporation to intentionally or recklessly facilitate, conceal or disguise in their accounting documents an occurrence of bribery, corruption or loss to a person that was not legitimately incurred. Importantly, proof that a benefit (not legitimately due) was actually received or given by the accused or another person is not required. This overcomes an evidentiary limitation that has historically been difficult for prosecutors to overcome, available at http://www.nortonrosefulbright.com/knowledge/publications/137893/new-false-accounting-offences-bolsters-bribery-toolbox-for-australian-federal-police.

It's personal: liability of senior executives under scrutiny

Senior managers who choose to turn a blind eye towards the corrupt practices of their companies and the employees they supervise may find themselves personally liable for allowing the company's books to be altered to conceal the corrupt nature of the payments made – even if it could not be shown that they had actually engaged in the payment of bribes.

The approach adopted by the SEC, which focuses on the complicity of senior executives and their failure to ensure that the company maintains accurate books and records and implements appropriate internal controls, should not be surprising in light of the memorandum titled *Individual Accountability for Corporate Wrongdoing* issued in September 2015 by the US Assistant Attorney General, Sally Yates, to all US Department of Justice (DOJ) prosecutors and civil litigators. The 'Yates Memo' is largely seen as a signal of intent by the DOJ to pursue and punish individuals for their role in corporate crime, in response to prior criticism that not enough had been done to hold individuals to account for their decisions which led to the financial crisis of 2007-2009.

This approach of targeting individuals in general, and senior executives in particular, was echoed in Singapore by Attorney-General VK Rajah SC (A-G Rajah) in an opinion editorial in November 2015, where he urged corporates to adopt a culture of compliance in order to combat commercial crime. In a portentous statement threatening to pierce the corporate veil, A-G Rajah warned that there was 'no certainty of escape from liability' for those seeking to hide behind complex corporate structures.

Senior management cannot act in conscious disregard or be wilfully blind to corrupt practices in their organizations. The specific targeting of individuals by the authorities, through the use of 'books and records' type and anti-money laundering offences, puts senior executives on notice of the need for them to prevent, detect and properly respond to corporate wrongdoing – and to set the right tone from the top.

As far as liability is concerned, this time it's personal

An earlier version of this article was first published on *Thomson Reuters Accelus Regulatory Intelligence and Compliance Complete*.

For more information contact:

Wilson Ang
Partner, Singapore
Tel +65 6309 5392
wilson.ang@nortonrosefulbright.com

Abigail McGregor
Partner, Melbourne
Tel +61 3 8686 6632
abigail.mcgregor@nortonrosefulbright.com

Paul Sumilas
Senior associate, Singapore
Tel +65 6309 5442
paul.sumilas@nortonrosefulbright.com

Jeremy Lua
Associate, Singapore
Tel +65 6309 5336
jeremy.lua@nortonrosefulbright.com

The World Bank Office of Suspension and Debarment reflects on lessons learned

"The World Bank Group is fully committed to its fiduciary responsibility to see that funds are used for their intended purpose: ending extreme poverty and boosting shared prosperity"

Jim Young Kim, President, World Bank Group

The World Bank's Report on Functions, Data and Lessons Learned (the Report), issued in the spring of 2016, explains the sanctions process adopted when a firm (or individual) involved in a World Bank-financed project is accused of a sanctionable practice, and reflects on lessons learned as the World Bank seeks to build a more transparent, fair and effective suspension and debarment system.

In the fiscal year ending June 30, 2015, the International Bank of Reconstruction and Development (IBRD) and the International Development Association (IDA), which together comprise the World Bank, committed US$42.5 billion in loans, grants, equity investments and guarantees to help promote economic growth and overcome poverty in developing countries. The World Bank has a fiduciary duty to ensure that the proceeds of these financings are used for their stipulated purpose. The sanctions system (as the suspension and debarment process is often called) excludes proven wrongdoers from operations financed by the World Bank and is a tool through which it seeks to enforce this duty.

The Report, and specifically the use of debarment as an effective sanctioning mechanism, should however be viewed in the wider context and as a reflection of a more general desire to supplement traditional monetary fines with other penalties. In addition to the World Bank, many governments and leading International Financial Institutions (IFIs) implement similar debarment procedures, as discussed in further detail below.

Sanctionable practices

The Report recognizes and defines five sanctionable practices as: fraud; corruption; collusion; obstruction; and coercion. Of the 303 sanctions cases brought before the Office of Suspension and Debarment (OSD) by the end of the 2015 fiscal year, the vast majority (83 per cent) related to a 'fraudulent practice', defined as "any act or omission, including a misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain a financial or other benefit or to avoid an obligation". According to the Report, most cases involved forged performance or experience documentation; forged bank guarantees or securities; or misrepresentation regarding past performance or experience. The OSD acknowledges in the Report that one of the key lessons learned in its 8 years of operation, is that fraudulent practices can be as damaging to development as corruption or collusion.

The process adopted by the World Bank

Where sanctionable practices are suspected, the Integrity Vice President (INT) will first conduct an initial fact-finding exercise. Where it believes there to be sufficient evidence of sanctionable misconduct, it will initiate proceedings by issuing a *Statement of Accusations and Evidence* (SAE) in relation to the accused firms or individuals (Respondent(s)) to the OSD. The OSD's Chief Suspension and Debarment Officer (SDO) will then thoroughly evaluate the information contained in the SAE and determine whether INT has presented 'sufficient evidence' that the Respondent engaged in the alleged sanctionable practice(s). If sufficient evidence is found, the SDO will issue a Notice of Sanctions Proceedings and formally notify the Respondent of the commencement of sanctions proceedings against it. The SDO will also recommend an appropriate sanction, which will be implemented unless the Respondent contests the allegations.

As such, the OSD is primarily designed to act as a check and balance and must impartially review the evidence before it. Since its inception, the OSD has referred 36 per cent of cases back to INT having determined that there was insufficient evidence to support one or more of the accusations made. However, only four per cent were rejected in their entirety.

One of the underlying objectives of the sanctions process is to ensure that it is fair to the Respondents and that they have the right to be heard. To this end, INT must disclose all relevant evidence including that which does not support its case. A Respondent has 30 days to submit a written explanation to OSD and 90 days to appeal the case to the World Bank's Sanction Board, which will review the case *de novo*. Having done so, the Sanctions Board will issue a fully reasoned decision stating whether it is 'more likely than not' that the Respondent engaged in sanctionable misconduct. If their finding is affirmative, it will then impose the appropriate sanctions having considered any mitigating or aggravating circumstances. According to the Report, appeals to the Sanctions Board were only made in 33 per cent of cases.

Sanctions

It is common for the OSD to impose a temporary suspension on a Respondent preventing it from entering into new contracts for World Bank financed projects whilst investigations are on-going. Whilst a temporary suspension is not announced publicly, it is posted on the World Bank's intranet and the Client Connection extranet site used by borrowing countries. It should be noted that, whilst the sanctions system is a 'quasi-judicial administrative process' – meaning that it does not have jurisdiction to enforce criminal or civil penalties – the World Bank may refer cases to national governments where the wrongdoing would likely be considered a criminal act.

Once the investigation has been concluded, and likely wrong doing established, there are five possible sanctions that may be implemented: debarment with conditional release; debarment for a fixed period (without conditional release); conditional non-debarment; public letter of reprimand and restitution. By far the most common sanction is debarment – meaning that the Respondent is declared ineligible to receive World Bank financed contracts. Where a debarment with 'conditional release' is granted, the conditions for release will focus on the debarred party demonstrating that it has in place, and has implemented for an adequate period, an integrity compliance program satisfactory to the World Bank (using standards reflective of global consensus). Debarments are public and printed on the World Bank's website.

As of June 30, 2015, the World Bank has publicly debarred or otherwise sanctioned more than 700 firms and individuals. Of the 368 cases concluded since the creation of the two-tier sanctions system in 2008, 39 per cent have been sanctioned during the last two fiscal years. The recent increase in suspension and debarment actions suggests the efficacy of the OSD's sanctions regime has improved and further demonstrates the World Bank's continued commitment in the fight against corruption.

This trend is reflected in the legislative changes in Canada, the EU and UK where the number of offences for which companies can be debarred has recently increased. In Canada, for example, amendments to the Public Works and Government Services Canada Supply Manual in 2014, mean that companies convicted of dishonesty offences (including bribery, extortion, forgery and insider dealing, as well as the offences under the Corruption of Foreign Public Officials Act) are prohibited from obtaining a federal government contract for a period of ten years, regardless of subsequent efforts to 'clean house' and remediate corrupt behaviors within the business. In contrast the UK imposes a maximum debarment of five years and enables companies convicted of a corruption or dishonesty offence to recover eligibility to bid for public contracts having undergone a 'self-cleaning' process.

Interestingly in the US, an upward trend in suspension and debarment actions has recently plateaued. The Interagency Suspension and Debarment Committee Annual Report, suggests that after consistent increases from 2009, the number of cases levelled off in 2015 with a slight decrease in reported instances of debarment from 1,929 in 2014 to 1,873 the following year. According to the Committee, this should not however be seen to reflect the effectiveness or otherwise of the system but regarded as 'purely a function of need'. Ultimately, Congress remains keen that the administrative powers of suspension and debarment are utilized where appropriate, a sentiment that is echoed in other quarters. The most recent OECD Foreign Bribery Report dated December 2014, for example, notes that out of 427 cases brought only two resulted in debarment and concluded that countries need to do more to ensure those that are sanctioned for having bribed a foreign public official are suspended from participation in national public procurement contracting.

Settlement

Following amendments to the sanctions system in 2010, cases before the World Bank may be resolved prior to, or during, sanctions proceedings by means of a negotiated resolution agreement or settlement. In these circumstances, the SDO's role is limited to reviewing the settlement to ensure it was entered into voluntarily, without duress and the agreed-upon sanction is broadly consistent with the Sanctioning Guidelines. The SDO may not modify the terms of the settlement in any respect. The proportion of cases concluded pursuant to settlement agreements has increased from 17 per cent to 21 per cent since the World Bank's first edition of this report in 2014, suggesting that the World Bank has become more open to Respondents seeking negotiated solutions.

Conclusion

The suspension and debarment system presents (as it is intended to) a significant deterrent for businesses particularly those that rely heavily on World Bank or government contracts. For those companies that do little else, a debarment may have a significant adverse impact on its ability to generate revenue. Debarment, as a sanction of choice, has a number of advantages. Not only does it act as a financial deterrent, it also excludes dishonest contractors from significant business transactions and sends an important message that sanctionable practices are not and will not be tolerated.

Whilst we expect the number of debarments imposed by the World Bank and government agencies to continue to rise, sanctions alone are not sufficient to combat the problem of fraud and corruption. As such these institutions would be advised to begin focussing more on incentives for cooperation in addition to the adoption of robust compliance measures.

Going forward, the World Bank is likely to continue to work with other multilateral development banks and organizations, as well as national governments. After all, the more rigorous those organizations and governments are in their pursuit of misconduct, the more straightforward the World Bank's own mission will be to ensure that its funds are used for their intended purpose.

In the meantime, the Report is an important tool for seeking to balance requirements of confidentiality with the need for transparency. To be effective, the OSD must retain its independence from external and internal pressures and must resist pressure to impose sanctions where there is insufficient evidence of wrongdoing.

For more information contact:

Sam Eastwood
Head of business ethics and anti-corruption
Partner, London
Tel +44 20 7444 2694
sam.eastwood@nortonrosefulbright.com

Holly Quinnen
Senior associate, London
Tel +44 20 7283 6000
holly.quinnen@nortonrosefulbright.com

Molly Seymour
Associate, London
Tel +44 20 7444 5877
molly.caddick@nortonrosefulbright.com

UK's second Deferred Prosecution Agreement

On Friday July 8, 2016, the second UK Deferred Prosecution Agreement (DPA) between the Serious Fraud Office (SFO) and a company anonymized as XYZ Limited (XYZ) was approved by the High Court. A redacted approved judgment was made available and the company has not been named, in all likelihood, because the individuals involved are being prosecuted and their later trial should not be prejudiced. In conjunction with the first DPA for Standard Bank in 2015, this case gives essential guidance on the new DPA regime.

The importance and form of voluntary cooperation

The key themes of engagement and co-operation chime with the judgment in Standard Bank.

Taking immediate action following the discovery of improper conduct again had considerable weight in gaining judicial approval for the DPA. With XYZ a law firm was retained within a week after concerns came to light and the SFO was orally informed less than a month later that a self-report may be made by an 'unidentified party'. The SFO was not made aware of the identity of the company for another five weeks or so. Similarly, with Standard Bank, a law firm was instructed within a week and the concerns were reported to the SFO within 30 days. The XYZ case therefore suggests that there is an acknowledgement on the part of the SFO that a firm will need to have some handle on the matter before making itself and the issue known to the SFO. No adverse comment was made about the first anonymous 'self-report' and may have some value. Equally a period of investigation of ten weeks from discovery may be considered an appropriate period before self-reporting. The key is the effective use of whatever time is taken.

After the notifications to the SFO were made, both XYZ and Standard Bank agreed to conduct internal investigations with the direction of the SFO in order to report back to the SFO within a period of around three months. The openness of the information provided thereafter was seen as fundamental to the DPA outcomes. Both companies provided oral summaries of first accounts of interviews, facilitated interviews with current employees and provided timely and complete responses to requests for information and material, save for those subject to proper claims of legal professional privilege. Further self-reports came out of the subsequent XYZ investigation phase. It is worth emphasizing that the cooperation by XYZ was described as 'exemplary'. No criticism was made of the company (nor indeed Standard Bank) in providing only oral summaries of first accounts rather than the first accounts themselves. Both companies were able to carry out their own initial internal investigation to understand the extent and facts of the wrongdoing without losing credit.

Parental responsibility

The financial penalties against XYZ include

- Disgorgement of gross profits of £6.2 million.
- A fine of £352,000.

£1.9 million of the disgorgement will be contributed by the company's US parent in repayment of dividends innocently received. The judgment makes it plain that there is no obligation on an innocent parent company to support a subsidiary in the financial obligations involved in satisfying a DPA and it therefore seems that XYZ's US parent has chosen to support XYZ for reputational reasons. The precedent may create additional reputational pressure for parent companies finding themselves faced with a similar situation in the future. In the words of the judgment, "a parent company receiving financial benefits arising from the unlawful conduct of a subsidiary (albeit unknown) must understand how this will be perceived." There may also have been good commercial reasons for the parent disgorging profit. Had the SFO not accepted lower fines for a DPA and prosecuted instead, the company would have been debarred from continuing to operate in the markets.

Mitigation and financial hardship

In the Standard Bank DPA, the gross profit was US$ 8.4 million multiplied by 300 per cent (the upper end of medium culpability) but reduced by a third due to the self-reporting and full cooperation with the SFO. In XYZ's case the court applied an uplift of 250 per cent to the gross profit of £6.5 million, arriving at £16.4 million, but reduced it by 50 per cent because it considered that XYZ's admissions were made "far in advance of the first reasonable opportunity" to do so. The court also justified such a discount "not least to encourage others how to conduct themselves when confronting criminality as XYZ has". One interpretation would be that the court was giving an additional discount (over the usual 30 per cent for an early admission) for a DPA. There has been pressure to include a higher discount for DPAs than for an early plea of guilty in a prosecution and this may be behind the decision in this case.

The court further reduced XYZ's fine to £352,000 because this was calculated to be the maximum amount that the company would be able to pay without risking insolvency. For the same reason, costs were not awarded to the SFO whereas Standard Bank had to pay around £300,000 towards the SFO's costs.

In reaching the reduced fine the court found it "relevant (as a measure of the commitment to improve and the extent of co-operation) that XYZ (with the financial assistance of ABC by way of further loan) has spent some £3.8 million in fees arising from the responsible steps it has taken through its own investigation, self-reporting, co-operating with the SFO and completing what might be described as a thorough 'self-cleansing' process". For companies (and their parents) in this situation this is notable as it acknowledges the importance of committing to a proper response upon discovery of an issue. The SFO's DPA Code of Practice for Prosecutors explicitly recognizes as public interest factors against prosecution: (1) a genuinely proactive approach adopted by the management team when the offending is brought to their notice, including taking remedial actions; and (2) the existence of a proactive corporate compliance program at the time of reporting.

First DPA for offences of substantive bribery

Both XYZ and Standard Bank were considered to have failed to have adequate procedures to prevent bribery under section 7 of the Bribery Act 2010. The potential draft indictment against XYZ however also related to offences of conspiracy to corrupt and bribe (under the old and new legislation). This was because the bribes were known to and authorized by senior executives who could be shown to represent the company's controlling mind. It was taken as a significant factor in the court's approval of the DPA that since identifying the misconduct the senior employees involved in the conduct were dismissed, seven suspect agents were terminated and bids for two suspect potential contracts were withdrawn. The court concluded that XYZ was a culturally different company to that which committed the offences.

The SFO's press release and final redacted judgment is available at https://www.sfo.gov.uk/2016/07/08/sfo-secures-second-dpa/.

For more information contact:

Neil O'May
Partner, London
Tel +44 20 7444 3499
neil.o'may@nortonrosefulbright.com

Andrew Wallis
Associate, London
Tel +44 20 7444 3443
andrew.wallis@nortonrosefulbright.com

Managing third party corruption risk

The legal issues raised by the engagement, monitoring and termination of third parties

"When a company discovers potential corruption issues with one of its active third parties, it faces a difficult balancing act between litigation, commercial and regulatory risks"

Third party service providers are businesses' single biggest corruption risk. The vast majority of prosecutions and regulatory settlements arise out of payments to agents, distributors, brokers, consultants, or other third parties.

Below, we highlight the key legal issues that commonly arise when an allegation of corruption is received in relation to an active third party and outline steps that can be taken when engaging third parties to enable companies to better deal with these legal issues as they develop.

What immediate steps should be taken by the company in the event of discovering an allegation in relation to a third party that it has engaged?

- Steps should be taken to determine the scope and nature of the issue, identify upcoming payments (outgoing and incoming) or other actions, ascertain its contractual rights, consider reporting obligations (internal and external) and preserve data as necessary.

Should payments be suspended while the company investigates the allegation?

- The seriousness of the allegation and associated regulatory risks needs to be balanced against the commercial risks of suspending payments.

Does the company need to self-report to financial/criminal authorities or seek consent to deal with potentially tainted funds?

- The company needs to consider early on whether it may need to self-report under applicable anti-bribery financial regulations or money laundering legislation – or whether it will want to seek consent to deal in potentially tainted funds to provide itself with a defence to money laundering offences. If so, this is likely to impact on the company's broader reporting strategy.

What should the company do if it does not discover specific evidence of corruption but has residual concerns about the third party?

- Consider re-running enhanced due diligence processes, including interviewing the third party face-to-face to determine whether to continue with the relationship and the risks of making future payments.
- Examine any contractual rights to information or to investigate.
- Suggest disclosing to the client that you have paid a third party and obtain their approval.

Should outstanding payments be made unless and until hard evidence of corruption is found?

- Hard evidence of corruption will rarely be unearthed during an internal investigation given the limitations on evidencing-gathering. The criminal and regulatory risks need to be carefully considered in light of the weight of the evidence and may override the civil risks of being sued.

How can a company determine whether the third party has provided genuine services for which it should be paid?

- Consider identifying an independent senior employee or advisor who can assess the value of the services provided and asking for evidence of those services.
- For 'introduction services' consider whether an introduction was truly necessary.

How should the company deal with any civil claim from the third party in relation to its fees in circumstances where there is strong evidence of corruption?

- Onsider a strategy of resisting payment until you have comfort that it is legitimate.

Does it assist to structure the payment as a settlement of a civil dispute as to the third party's fees?

- Structuring any payment as a settlement does not in itself mitigate the risk of making payment: what is important is the reality of the services for which payment is to be provided.

Positive steps that can be taken

Contractual provisions are important in terms of providing tools to deal with the legal issues arising out third party engagement. Ideally, a company should aim to give itself rights to

- Audit and investigate issues and suspend payments while doing so.

- Terminate and withhold outstanding payments on the basis of non-cooperation or breach of the company's ABC policy.

For more information contact:

Sam Eastwood
Head of business ethics and anti-corruption
Partner, London
Tel +44 20 7444 2694
sam.eastwood@nortonrosefulbright.com

Ruth Cowley
Partner, London
Tel +44 20 7444 3396
ruth.cowley@nortonrosefulbright.com

Jason Hungerford
Partner, London
Tel +44 20 7444 2474
jason.hungerford@nortonrosefulbright.com

James Thomas
Senior associate, London
Tel +44 20 7444 2470
james.thomas@nortonrosefulbright.com

Andrew Reeves
Associate, London
Tel +44 20 7444 3138
andrew.reeves@nortonrosefulbright.com

Does it work: testing and assurance of compliance programs

"The DOJ and SEC have no formulaic requirements regarding compliance programs. Rather, they [ask] three basic questions: Is the company's compliance program well designed? Is it being applied in good faith? Does it work?" (DOJ/SEC Resource Guide to the FCPA)

Multinational companies have invested heavily in ethics and compliance programs in recent years, in response to accelerating regulatory enforcement and high-profile investigations: Petrobras, FIFA, VW and so on. While US and UK regulators have given clear guidance – supported by consistent guidance from the United Nations, World Bank, Transparency International and others – most corporates have largely neglected the requirement that, to be effective, compliance programs must periodically be tested. Companies new to modern ethics and compliance programs rightly focus on developing policies, procedures and training, but in short order those measures should be assessed and tested.

Why test?

Ethics and compliance programs have two primary purposes:

- First, to actually reduce the risk that improper behavior may occur.
- Second, to provide a serious and credible response (to regulators, to shareholders, to customers and business partners and to the public) if improper behavior occurs, notwithstanding the company's best efforts.

A failure to test the effectiveness of a compliance program guarantees that neither goal will be fully realized. Failing to test or monitor the program means that weaknesses in its design or implementation are unlikely to be identified and remediated until it is too late. A failure to test or monitor the program also devalues it in the eyes of regulators, particularly where an issue arises in an area of weakness that could have been previously identified and remediated. This can have serious implications: prosecutors will be more likely to pursue a case, and less likely to give the company credit for their compliance program. Under the UK Bribery Act, that means potentially not qualifying for the section 7 'adequate procedures' defence: 'monitoring and review', encompassing both internal and external verification, is one of six principles set out by the Ministry of Justice in its 'outcome focussed' assessment of a corporate's compliance program. Similarly, US Federal Sentencing Guidelines make clear that, along with self-reporting and cooperation, the key factor "that mitigate[s] the ultimate punishment of an organization [is] the existence of an effective compliance and ethics program … including monitoring and auditing to detect criminal conduct [and evaluating] … periodically the effectiveness of the organization's compliance and ethics program".

Done right, systematic and periodic testing, monitoring and reinforcement processes not only mitigate risk, but also have major benefits in driving the effectiveness and efficiency of a compliance program. Testing and monitoring helps to identify areas for improvement before more costly issues arise and helps to root out inefficiencies or inconsistencies. Testing can also drive effective implementation and provide a significant deterrent: if, for example, employees know that a sample of expenses or gifts and entertainment records will be reviewed, it is likely to encourage them to abide by company policy and follow proscribed procedures and controls. Testing and monitoring also provides valuable management information that senior personnel can assess in discharging their responsibilities to ensure that compliance risks are properly managed.

Done wrong, 'certification' can be dangerous. Many companies have sought 'certification' from external consultants that they have in place a compliance program. Such certification is of limited value because what needs to be tested – and what regulators are interested in – is whether the program is effective, not whether it exists.

"A good compliance program should constantly evolve … compliance programs that do not just exist on paper but are followed in practice will inevitably uncover compliance weaknesses and require enhancements. Consequently, DOJ and SEC evaluate whether companies regularly review and improve their compliance programs and not allow them to become stale … An organization should take the time to review and test its controls, and it should think critically about its potential weaknesses and risk areas." DOJ/SEC Resource Guide to the FCPA

How?

"Commercial organizations will … wish to consider how to monitor and evaluate the effectiveness of their procedures and adapt them where necessary … Organizations could… consider formal periodic reviews and reports for top-level management… [and] seeking some form of external verification or assurance of the effectiveness of procedures" *Ministry of Justice UK Bribery Act Adequate Procedures Guidance*

Monitoring and testing should follow a systematic and risk-based methodology. It should be conducted periodically by individuals independent from the matters reviewed. A hybrid team of company personnel (from audit, legal and/or compliance, and possibly with representatives from the business) and outside advisors ensures that the company's internal team benefits by learning the review process, whilst receiving the outside perspective of experts who have experience across a range of companies and sectors. Such an approach also leverages the company's existing resources, helping to control external costs.

The scope, methodology and results of the review should be carefully recorded. The exact nature of the monitoring will vary depending on the company's structure and the risks relevant to it, but reviews can include some or all of the elements set out below.

First, the framework, content and ownership of policies and associated training should be reviewed on a periodic basis. This review provides a systematic check that policies and training are up-to-date with legal requirements, properly owned by an appropriate individual or team, and ensures consistency as between various policies.

Second, a sample set of recent transactions should be tested. This is likely to involve a combined review of accounts, supporting documentation and interviews. This is not primarily a matter of auditing compliance with internal procedures, but rather a substantive review to identify strengths and weaknesses of existing processes and controls, deficiencies in comprehension and to detect broader issues for remediation. Such an assessment adds rigour to and supplements the company's ongoing risk assessment process. This is particularly suitable for higher-risk third parties, markets and transactions and/or as a periodic in-depth review on a rolling market-by-market basis.

Third, comprehension of legal requirements, risk factors and ethical responses should be tested. For the general employee population, this usually means evaluating the uptake from your existing training program and making improvements where appropriate. For senior managers, more sophisticated exercises can be used to assess whether proper 'tone from the top' is being set, which can inform broader strategy discussions.

Testing and assurance is not an optional bolt-on, a 'nice to have': it is a fundamental requirement for an effective ethics and compliance program that meets regulatory expectations. It is also not merely a matter of determining whether processes are being followed: it is ensuring that policies and standards are understood and being met on a daily basis, and that employees are well-equipped to make the right decisions. Put another way, testing ensures that the company's ethics and compliance program really works, and that it continues to work as its business changes and grows.

For more information contact:

Jason Hungerford
Partner, London
Tel +44 20 7444 2474
jason.hungerford@nortonrosefulbright.com

Andrew Reeves
Associate, London
Tel +44 20 7444 3138
andrew.reeves@nortonrosefulbright.com

Compliance due diligence from a company perspective – An interview with Roland Kemper, DEKRA SE

Roland Kemper, 40, is a senior counsel in DEKRA SE's Legal & Compliance department. DEKRA is an international provider of testing, inspection, and certification services. Roland focuses on the legal side of M&A projects and on corporate governance matters. In addition, he is a non-executive member of DEKRA's management holdings in the UK, the US, and Denmark. Roland is a law graduate (University of Bonn, The George Washington University Law School, King's College London) and a management graduate (FU Hagen, LSE). He is admitted to the New York State Bar and to the German Bar.

Compliance has received ever more attention in the last few years. This is particularly so when it comes to acquiring a company in relation to which a compliance due diligence has evolved significantly. How is this handled at DEKRA?

DEKRA carries out a compliance due diligence in every acquisition process, with varying intensity of course. In the last ten years, acquisitions have played a major role in accelerating DEKRA's growth in the testing, inspection, and certification business (TIC). Generally, these acquisitions have targeted companies outside of DEKRA's German home market. In recent years, DEKRA acquired, for instance, the AT4 Wireless, a group headquartered in Spain and with subsidiaries in Taiwan, Chile, and in the US, and QuieTek Corporation in Taiwan, and the Scottish company Optimus Seventh Generation, a provider of safety consultancy services to oil platforms. Again in Taiwan, DEKRA formed a joint venture company in 2015 for 'electromagnetic compatibility testing' together with the iST Group. Transactions hence often involve jurisdictional and cultural contexts that may not be well-known to the in-house legal counsel. And for this reason, it is even more important to engage in due diligence that covers compliance aspects as well.

What does a standard compliance due diligence at DEKRA look like?

As a matter of principle, in-house legal counsel at DEKRA must involve themselves heavily in the legal due diligence process on the basis of the experience they gain in advising the operative business. Further, each DEKRA in-house legal counsel is called upon to integrate the compliance perspective into every step of the advisory process, be it in an operations or transactional context. If they lack the required knowledge or experience to deal with a certain compliance issue, or if a conflict of interest arises, we expect them to take the initiative and involve the Group's Compliance Office and, if needed, outside counsel.

As to the depth of, and the aspects covered by, the standard compliance due diligence process, it is necessary to remember that DEKRA's core expertise consists in delivering TIC services. TIC services mean that DEKRA assesses whether products, appliances, and processes comply with certain standards. These standards regularly relate to features that express the technical safety or the quality of the product, appliance or process at issue. In fact, DEKRA's historical core business is ensuring the road safety of trucks and cars. More generally, these standards may be regulatory standards imposed by governmental agencies or they may be standards that are related to certain industries. Often, the authority assessing compliance with such standards depends on the respective DEKRA company being specifically accredited. For instance, DEKRA's Product Certification service unit is specifically accredited under the *European Electromagnetic Compatibility Directive 2014/30EU* (EMC) to assess whether devices that contain an electrical energy source interfere with the operation of other products or are affected by themselves by the operation of other products. Another example is the periodic safety testing of trucks and cars in France, Germany and Sweden. In these countries, the state has delegated DEKRA the authority to assess whether trucks and cars comply with certain road safety standards. It is paramount for DEKRA to ensure compliance with all aspects of the law. Governmental and non-governmental accreditation bodies are key stakeholders for DEKRA. Consequently, our compliance due diligence always covers all areas that may be deemed as compliance relevant.

In your practice, which are the areas that are generally compliance relevant and hence a main part in your compliance due diligence?

Depending on the nature, size, and location of the business conducted by the target company, we investigate certain areas more intensely. For instance, if the target conducts its business in regions with a low ranking on Transparency International's Corruption Perception Index and works with freelance sales agents in order to enlarge its customer base, we will heavily emphasise anti-bribery aspects. Here, we take into account specific compliance requirements set out in laws such as the US Foreign Corrupt Practices Act and the UK Bribery Act. On the other hand, the structure, home jurisdiction and place of business of our target companies' shareholders, as well as the target companies' financing and payment arrangements, are usually very straightforward. Hence, we would not initially focus on anti-money laundering as much as you would do in settings that are more susceptible or in the financial services industry. DEKRA's target companies are mostly in the small to mid-size range and privately held. As a result of this, tax compliance is an important topic, and DEKRA's in-house legal counsel will closely cooperate with the tax department and external tax specialists to minimize DEKRA's exposure to legal and reputational risks stemming from tax law violations.

Does DEKRA's compliance due diligence also comprise a review of compliance with industry specific standards which go beyond the legal requirements?

Yes, it does, and that is a consequence of how DEKRA positions itself in the market. Being a 'neutral third-party' provider of TIC services lies at the heart of DEKRA's identity. Integrity is one of DEKRA's five core 'people values'. In addition, DEKRA's 'Vision 2025' is to 'be the global partner for a safe world'. Part of this positioning is that most of DEKRA's TIC services actually contribute to reducing the risk of accidents at work, in traffic and at home as well as to change conditions that lead to health impairments. In line with this positioning, our compliance due diligence always assesses whether the target company has had employment, safety or environmental issues. You asked about industry specific standards: DEKRA indeed is a member of TIC specific trade associations and, in particular, the International Federation of Inspection Agencies (IFIA). The IFIA has a set of compliance principles that binds its members which are broader than what is required by law. In addition to reviewing whether a target company has complied with certain standards in the past, however, we use the compliance due diligence process to really understand whether the target company's organizational culture supports a mindset that tries to minimize issues like employment safety incidents. We invest a lot of effort in understanding the target company's attitude to safety.

What time period do you generally cover in your compliance due diligence?

While the statute of limitations provided in applicable laws tends to frame our scope of attention, we try to fully exhaust the information available publicly, in the data room and delivered in management meetings. This is not only a question of diligence or thoroughness. DEKRA's business is not heavy in physical assets. Quite to the contrary, the success of DEKRA's business largely hinges on DEKRA's reputation as an independent and neutral third-party provider of TIC services. This reputation materializes in the daily behavior of DEKRA's employees and in how the market participants perceive DEKRA's brand. Consequently, it is very important for DEKRA to ascertain that the target company's organizational culture and the behavior of its leadership is such that the target aligns with DEKRA's reputational demands. Because of this need for alignment, we look at any available piece of information, irrespective of its age, that may cast a doubt on this potential alignment.

How and with what kind of focus do you review the target's existing compliance management system?

In order to understand whether a target company has implemented and oversees an adequate compliance management system, we try to understand how the target company's leadership defines what the risks to the company are and how the target company's leadership describes the management systems put in place to tackle such risks. That said, it is DEKRA's stance that a well-designed compliance management system must be the result of an integrated concept of risk management and internal controls. At the end of the day, compliance risks have the potential to become business risks. Thus, the scope of attention to the compliance management system naturally overlaps with and is part and parcel of a company's risk management and controls system. In addition, all owners of potential compliance risks, in particular the leaders of the operational units, must be involved in such an integrated risk and compliance management system. In order to test such involvement, and depending on the size of the target company, we look at whether the company has appointed compliance officers across service units and functional units who report compliance matters to a top compliance officer. We also try to understand whether such formal organization is brought to life by specific measures- e.g. regular interviews between the compliance officers, regular training, regular town hall meetings, annual 'compliance leadership dialogues', ad-hoc compliance audits, and an appropriate level of documentation. Certainly, we try to understand whether the top compliance officer has been formally designated to receive whistleblower messages or whether there is a hotline or external ombudsman. As already said, we find it very important to understand whether the target company has an organizational culture that fosters compliance with the law, integrity and respect for the rule of law and, thus, buttresses the rather formal compliance measures mentioned previously.

What is DEKRA's general approach in a compliance due diligence? Do you proceed in a step-by-step approach and if yes, what are the respective steps?

In terms of our practical approach to compliance due diligence, we certainly recognise that we have to follow the customary systematic approach whereby the level of intensity of compliance due diligence increases as the transaction proceeds to completion. Within the initial stage of the transaction process, which may start even before the conclusion of a non-disclosure agreement, we try to categorise certain compliance risks, e.g. corruption, based on indicators that may have become apparent or are public anyway. E.g. do the company's shareholders have links to public officials? Is the target company located or doing business in a jurisdiction with significant institutional voids? What is the target company's record in online and other publicly available media? That said, we make a preliminary assessment of compliance risks and try to identify potential red flags even before we initiate more formal due diligence investigations. The heavy lifting of compliance due diligence then takes place before we sign a definitive agreement, which implies the use of outside counsel and other external specialists. Such heavy lifting regularly involves active communication to the target company's leadership. Here, in-house legal counsel jointly with outside counsel and relevant operational leadership at DEKRA interview the target company's leadership as well as certain members of middle management in face-to-face interviews that take place as part of the 'management meetings'. In exceptional circumstances, DEKRA might insist at this stage that the target company's leadership discloses certain internal communications that surround incidents that DEKRA perceives as potential compliance risks. Depending on the weight and type of the compliance risks identified, DEKRA may also decide prior to completion that it will engage in certain post-completion compliance investigations spearheaded by the Legal & Compliance department. Irrespective of whether we have been able to identify certain compliance risks prior to completion and in line with DEKRA's insistence on integrated risk and compliance management systems, DEKRA's audit department regularly runs audits on all subsidiaries and, hence, the newly acquired business.

How are the findings of your compliance due diligence generally taken into account in the negotiations and the transaction documentation?

DEKRA's business model largely hinges, as already outlined, on the integrity of DEKRA's employees, the perception of DEKRA's brand by market participants and on DEKRA's reputation as a neutral, independent third party provider of TIC services. DEKRA's approach to compliance risks is that it avoids acquiring target companies with a compliance history that have the potential to infect DEKRA's reputation. Having said this, inserting compliance related representations, warranties, and specific indemnities into the definitive agreement is only a minimum requirement. Generally, DEKRA will acquire a company only if DEKRA's compliance experts have strong reason to believe that compliance risks will not materialise at all or beyond of what is already known. Sometimes a carve-out can help, especially if the target company has various service lines that conflict with the TIC idea. If, in exceptional cases, the 'heavy lifting' of the compliance due diligence mentioned above could not sufficiently ascertain a potential compliance risk or the extent of a risk partly materialized, we may either abstain from the transaction or insist on having the right to rescind the transaction or reduce the purchase price ex-post. Reducing the purchase price may already be part of the purchase price mechanism in 'staggered acquisitions' where DEKRA has partly bought out the management/owners. Here, the right to purchase further shares later on will include a pricing model that reflects an impact of compliance risks should these materialise.

How do you make use of the findings of the compliance due diligence when integrating the target company into the DEKRA group?

Any results of compliance due diligence that indicate a relevant level of risk will be used to inform risk mitigation measures. The clear message to any target company's leadership is that DEKRA will make no concessions when it comes to its five core people values. As indicated earlier, integrity is one of these principles. Even if compliance due diligence does not uncover distinct compliance risks, it will help DEKRA to assess the costs, time, and effort related to the integration of the target company into the Group's compliance management and into the Group's compliance culture.

For more information contact:

Nicolas Daamen
Of counsel, Munich
Tel +49 89 212148 346
nicolas.daamen@nortonrosefulbright.com

Michael Gaul
Associate, Munich
Tel +49 89 212148 308
michael.gaul@nortonrosefulbright.com

Compliance due diligence in Germany

The assessment of compliance risks in connection with legal due diligence upon the acquisition of a company is increasingly becoming market standard in Germany. Proceeding without a compliance check is hardly conceivable – not only in larger corporate transactions but also in small and mid-size transactions. One of the reasons for this trend is that, in accordance with the business judgment rule which is also applicable to companies in Germany, the purchaser's management is obliged to evaluate all available information and to exploit sources of information in all important managerial decisions within reasonable limits. Due to the complex nature of corporate transactions as well as the economic significance of compliance risks for the target group and the purchaser, it is in almost all cases necessary to address compliance issues in the course of due diligence assessments.

This article seeks to provide an overview of the standards which have evolved over time as well as new trends and developments in connection with compliance due diligence processes in Germany.

Compliance risks connected to company acquisitions

When acquiring a company, the purchaser faces a number of different compliance risks. These include, in particular, corruption and bribery by management or employees of the target group as well as breaches of the following regulations

- Competition and antitrust law
- Procurement law
- Data protection law
- Customs and foreign trade regulations.

Nevertheless, there is a tendency in Germany not to devote the same amount of attention to all potential breaches when checking such breaches against the aforementioned legal provisions in the course of compliance due diligence procedures. In many cases, risk assessment is limited to corruption and breaches of antitrust law, as sanctions for misconduct in these areas are often the most severe. Furthermore, companies are mindful that they can be excluded from public procurement and tenders due to corruption offences and thus will additionally suffer considerable reputational damage.

In-depth assessment of corruption risks

Whilst the scope of assessment is often focused on corruption and breaches of antitrust law, the extent of assessment of these areas have increased significantly. This is particularly relevant for dealing with corruption risks. The trend is triggered by the increasingly strict prosecution and sanctions practice implemented by German authorities, which not only targets large company groups but also extends to medium-sized companies, as is clear from recent enforcement patterns.

Process of compliance due diligence

In Germany, there are two concepts for the organization of compliance due diligence: there is a three step approach in which the compliance due diligence is carried out in three phases: pre-signing, post-signing and post-closing. Alternatively, there is a two-step approach in which the assessment is limited to the pre-signing and post-closing phases.

The two step approach seems to have gained a foothold on the market.

The three step approach is only applied in exceptional cases and is usually limited to those in which possible compliance risks have been identified during the pre-signing due diligence which need to be clarified further before closing. At the same time, the identified compliance risks must not be so severe as to be a deal breaker to the signing. Thus, the scope of application for a three step approach is conceivably narrow.

Pre-signing compliance due diligence

With regard to the pre-signing phase, the compliance due diligence process is usually limited to a desktop review and risk analysis. In this context, the target group's existing compliance management system as well as the respective report and control lines are checked with regard to key measures, e.g. code of conduct, policies, organization chart of compliance structure, identification and competence of compliance officers, etc. This enables the purchaser to make a preliminary assessment of whether compliance is an unknown concept for the target group or if management and employees have at least a general awareness of compliance.

Furthermore, there is an increasing trend in which the purchaser tries to use compliance expert sessions with the seller's (or target group's) compliance officers to help the purchaser develop an increased sensitivity for identifying possible compliance risks in the target group.

Post-closing compliance due diligence

During the post-closing phase, the purchaser is mainly confronted with two challenges

First, the target group has to be integrated into the purchaser's compliance management system by adapting the report and control lines and by transferring the purchaser's compliance standards to the target group.

Secondly, possible compliance risk issues, which are substantially based on the results of pre-signing compliance due diligence, have to be clarified further. In this case, a more extensive post-closing compliance due diligence is required if it transpires during the pre-signing due diligence that the target group does not have a functioning compliance management system or that there are specific indications of compliance breaches. In practice, the trend focuses on the areas of corruption and antitrust law.

In case of continuation of possible corruptive practices after closing, German law provides not only for a continued liability on the part of the target group and its management but also for administrative offence law liability on the part of the purchaser.

Principles of compliance risk implementation in sale and purchase agreement

Compliance risks are usually incorporated into the sale and purchase agreement in two ways: an indemnification clause between seller and purchaser is agreed with regard to known risks, or, for unknown risks, the seller gives a guarantee.

Thus, with regard to the liability regime in a sale and purchase agreement, the purchaser benefits from pre-signing compliance due diligence. Where specific risks have been clearly identified by way of a pre-signing assessment, the seller will agree to issue an indemnity for such risks. Otherwise, the seller will only provide the purchaser with a compliance guarantee. From the purchaser's perspective, the clear benefit of an indemnity over a guarantee is that an indemnity is usually not subject to the same restrictive limitations as a guarantee (e.g. de minimis, threshold, cap, limitation period). As a rule, an indemnity is granted on the basis of a 1-to-1 Euro compensation for occurred damages, hence no de minimis or threshold, and normally with a deviating cap and a longer limitation period than the guarantee claims.

Further, a guarantee has a narrower scope than an indemnification. In the currently prevailing seller-friendly market environment in Germany, the seller will not be prepared to assure that the target group is not in breach of any and all material regulations and laws. The market trend rather suggests that the seller will only guarantee compliance with the German anti-corruption laws (and, if applicable, with the FCPA and UK Bribery Act) in the framework of a compliance guarantee.

Problems and tendencies in contract implementation

One of the outstanding issues with regard to contract implementation is the legal consequence of an infringement of a compliance guarantee. Compensation for lost profits (e.g. exclusion from public tenders) as well as for internal administrative costs and external advisers' fees (e.g. legal advice and court costs regarding internal investigations) are often excluded in the sale and purchase agreement. Furthermore, any reputational damage incurred is hard to measure in numbers which means that, due to strict legal consequences, the compliance guarantee is only of limited value when it comes to effectively protecting the purchaser. However, it remains to be seen whether there will be changes to this trend in the current market standard in Germany.

There is an increasing trend among W&I insurers – depending on the thoroughness of the due diligence and the scope of the compliance guarantee – to insure compliance guarantees, especially in connection with corruption and bribery. Concluding a W&I insurance often constitutes a sensible possibility for reaching an agreement, although the seller is not prepared or only prepared to

cover compliance risks up to a certain amount- an option with which the purchaser may not accept.

Conclusion

Compliance due diligence procedures have become market standard in Germany for every large transaction. In the case of medium-sized and smaller transactions, compliance due diligence is becoming more common, depending on the target group's industry. The criteria regarding the scope of assessment, the procedure and the depth of assessment are becoming increasingly standardised. Such criteria are

- Content-based focus on corruption and anti-trust risks.
- Implementation of compliance due diligence in two phases: pre-signing and post-closing.
- The pre-signing compliance due diligence is limited to a desktop review, risk analysis and (increasingly becoming more common) compliance expert sessions.
- The post-closing compliance due diligence has the aim of an in-depth analysis of possible compliance risks identified in the course of the pre-signing due diligence.
- Taking on guarantees and indemnities for compliance/ corruption risks in SPAs.
- Hedging compliance/corruption risks by W&I insurance.

For more information contact:

Nicolas Daamen
Of counsel, Munich
Tel +49 89 212148 346
nicolas.daamen@nortonrosefulbright.com

Michael Gaul
Associate, Munich
Tel +49 89 212148 308
michael.gaul@nortonrosefulbright.com

Bribery and public policy in the English courts

In *National Iranian Oil Company v Crescent Petroleum* [2016] EWHC 510 (Comm), the High Court held that the court would not, as a matter of English public policy, refuse to enforce a contract procured by bribery. The decision provides a reminder that notwithstanding the English courts' apparent willingness to provide a remedy to victims of bribery and corruption, the courts will still operate in accordance with established legal principles.

The legal landscape

As Lord Neuberger stated in *FHR v Cedar* [2014] UKSC 45, "… concern about bribery and corruption generally has never been greater than it is now … Accordingly, one would expect the law to be particularly stringent in relation to a claim against an agent who has received a bribe or secret commission." The case is one of several recent decisions in which the victim of bribery or corruption has sought a remedy in English civil proceedings.

In the FHR case, the Supreme Court confirmed that where an agent has received a bribe or secret commission in breach of its fiduciary duty, not only must the agent account to the principal for the secret commission, but the principal has a proprietary claim to it – thereby strengthening of the principal's rights as against an agent in such circumstances.

National Iranian Oil Company v Crescent Petroleum

The proceedings in *National Iranian Oil Company v Crescent Petroleum* arose out of a long term gas supply contract. It was alleged by Crescent that NIOC had failed to deliver any gas in breach of the terms of the agreement. Crescent began arbitration proceedings and obtained an award. In the course of the arbitration it was argued by NIOC that the claim should not succeed because the underlying contract had been procured by corruption. However, after hearing the evidence, the tribunal ultimately rejected the corruption argument.

Subsequently, NIOC applied to set aside the arbitration award under section 68 of the Arbitration Act on the grounds of serious irregularity (specifically section 68(2)(g): "the award or the way in which it was procured being contrary to public policy"), again relying on the previous allegations of corruption.

The court's decision

The application ultimately failed on the basis that, as the tribunal had previously found, the underlying contract had not been procured by corruption.

The court also rejected NIOC's alternative submission that the agreement was nevertheless 'tainted' by corruption. In support of this argument, NIOC had contended that public policy and legislative approach had hardened had in recent years hardened against bribery and corruption such that a court would not now take the same view as suggested at first instance in *Westacre Investments v Jugoimport-SPDR* [1999] QB 740, namely that the public policy of sustaining international arbitration awards outweighed the public policy in discouraging international commercial corruption.

However, even if recent case law has marked a policy shift to act even more robustly against bribery and corruption, a mere suggestion that a contract has been 'tainted' without further evidence, cannot be enough. As Burton J concluded, to introduce a concept of tainting of an otherwise legal contract would create uncertainty, and would in any event wholly undermine party autonomy. There may be many contracts which have been preceded by undesirable conduct on one side or other or both, such as lies, fraud or threats. However, the Court will not interfere with such a contract unless: (i) the contract itself was illegal and unenforceable; or (ii) one or more of the acts induced the contract, in which case it might be voidable at the instance of an innocent party. The Judge went so far as to say that this would be the case even if one or more of those parties had committed criminal acts for which they could be prosecuted.

Of perhaps greater significance, the court held that even if a different conclusion had been reached on the facts, there is no English public policy that requires a court to refuse to enforce a contract procured by bribery. This fits with the principle that contracts procured by bribery are voidable rather than void and so a court might decide to enforce such a contract at the instance of one of the parties.

In reaching the above decision, Burton J set out various conclusions

- "English public policy applies so as to lead a court to refuse to enforce an illegal contract, even if not illegal at relevant foreign law, such as a contract to pay a bribe." However, in the present case, the contract in question was not an illegal contract.
- With regard to bribery, there "is no English public policy requiring a court to refuse to enforce a contract procured by bribery. A court might decide to enforce the contract at the instance of one of the parties. It is not that the contract is unenforceable by reason of public policy, but that the public policy impact would not relate to the contract but to the conduct of one party or the other."
- In particular, there is "no English public policy to refuse to enforce a contract which has been preceded, and is unaffected, by a failed attempt to bribe, on the basis that such contract, or one or more of the parties to it, have allegedly been tainted by the precedent conduct."
- In any event in the present case, the tribunal had concluded that the contract in question had not been procured by bribery after full consideration and evidence. The court should not interfere with the tribunal's decision save where there is fresh evidence or in very exceptional circumstances – neither of which existed in the present case.

Commentary

As a matter of law, the decision must be correct insofar as it accords with the established principle that contracts procured by bribery are voidable rather than void. Nevertheless, insofar as recent cases had shown a trend to provide a remedy to victims of bribery where possible, this decision provides a sobering reminder that the courts will and must operate in accordance with established legal principles.

For more information contact:

Andrew Sheftel
Senior knowledge lawyer
Tel +44 20 7444 5682
andrew.sheftel@nortonrosefulbright.com

Exploring human rights due diligence

Executive summary of a human rights due diligence project run by Norton Rose Fulbright and British Institute for International and Comparative Law

Business and human rights represents an evolving area of risk for businesses which is assuming an increasingly legal dimension. As in many other areas, the prudent response is due diligence. Indeed, many businesses already conduct due diligence in a variety of contexts, including mergers & acquisitions and project finance. However, the nature of human rights due diligence is different from the due diligence that companies are used to conducting.

The UN Guiding Principles on Business and Human Rights (the Guiding Principles) set out the components of human rights due diligence. Recognizing the unique characteristics of human rights due diligence is fundamental to the effective identification and management of human rights impacts which may be associated with a business' operations, supply chains or value chains.

Although much has been written about human rights due diligence, there is still a lack of clarity about what is required amongst many businesses. Further guidance is needed to help businesses understand the scope, meaning and consequences of human rights due diligence as described in the Guiding Principles.

With this in mind, Norton Rose Fulbright and the British Institute of International and Comparative Law decided to collaborate on a joint study (the Study) comprising academic research, an anonymous survey and interviews with business representatives, with the aim of clarifying issues of law, principle and practice in the area of human rights due diligence.

Our study

- Clarifies the meaning and scope of human rights due diligence.
- Examines its legal basis, developments and underlying requirements.
- Analyses the actual practice currently undertaken by companies through the lens of the core elements of the Guiding Principles.

The primary purpose of the Study is to provide practical recommendations for businesses in relation to their approach to human rights due diligence. The key findings from our Study are set out in this summary briefing, while a detailed 15,000 word peer reviewed article will appear in a forthcoming edition of the *Business and Human Rights Journal* published by Cambridge University Press.

On October 17, 2016, Norton Rose Fulbright in collaboration with the British Institute of International Comparative Law hosted a forum on human rights due diligence which explored good practices and challenges for business enterprises.

The forum discussed the findings of a report released by Norton Rose Fulbright and the British Institute of International and Comparative Law on human rights due diligence. The speakers and audience were made up of legal professionals, academics and representatives of businesses and international organizations.

Key takeaways

The following are the key takeaways from the forum.

- Why conduct human rights due diligence: The top incentives for conducting human rights due diligence include brand, reputation, corporate legal risk avoidance and compliance with reporting requirements and applicable laws.
- Focus due diligence on human rights impacts: Focusing due diligence on the impact of the business enterprise on human rights is the best way to implement the United Nations Guiding Principles on Business and Human Rights (UNGPs). Only those businesses which had undertaken specific human rights due diligence processes had identified a significant number of human rights impacts.

- Corporate perspective: When conducting human rights due diligence, companies need to look beyond the impact on the enterprise to the impact on the affected rights holder, as a stakeholder. This means that when conducting human rights due diligence, the concept of ‘materiality’, so ingrained into the mind-set of corporations, is superseded by the actual and potential impact on stakeholders.

- Mind the gap: Normal corporate processes such as audit and record keeping are not usually effective in revealing the impact of the business enterprise on human rights. The board of directors and the C-Suite need to dig deeper and conduct specific human rights due diligence in order to bridge the gap between what is being reported and the reality. They also need to ensure that the legal function undertakes careful verification of companies’ public statements. These steps will serve to mitigate potential liability for actual adverse human rights impacts.

- Nature of the modern corporate group: Global businesses should be aware that there is an increasing trend for companies in countries such as the UK, Canada, Germany and the US to suffer reputational damage and sometimes even legal action because of the acts of their subsidiaries or subcontractors abroad. An enterprise can no longer just look at its own business. It needs to make sure that proper systems and processes are in place in other companies in the group. It also needs to understand the human rights impacts of other businesses within its supply and value chains.

- Cross-departmental approach: In order to have a better understanding of their human rights impacts, business enterprises need to get away from the modern corporate structure where each department is working in a silo and concentrates on its own specific mandate. Human rights due diligence is most effective when it is cross-departmental. To get the best results, a combination of legal, compliance, human resources, procurement and corporate social responsibility teams is desirable.

- Roles, responsibilities and objectives: Human rights is not an ‘add-on’ feature of the organization but should be central to the business strategy. Consequently, it is the responsibility of the board to identify, own, manage and mitigate risks. This means that risk owners need to be clearly identified, resources need to be targeted to the most significant risks and controls, and prevention activities should align with any changes in the risk profile of the organization. The objective of leaders at all levels across the organization should be to build a culture where human rights are respected.

- Look back principle: The law is developing and in many years to come businesses could be held to account for their actions today. For this reason, it is not enough to look only at where the law is now; businesses need to look at the direction in which the law is travelling to influence their current behavior, the so-called ‘look back principle’, which has already been applied in other areas like anti-bribery and corruption and tax avoidance. In the sphere of business and human rights, it would seem that the courts are moving towards enforcing higher standards than those currently set out in the black letter law, so companies should look to these standards as their guiding point.

- Voluntary principles treated as hard law: When determining what standard of due diligence is necessary, it can be helpful to look at the UNGPs, the leading soft law in this area. Although these principles are voluntary, courts are starting to mention these Principles in their rulings.

- An effective system without budget is a myth: It is not enough to ask lawyers to draft human rights policies and risk assessments if there is no budget allocated to the implementation, training and enforcement of these. A business enterprise which is serious about assessing and improving its impacts on human rights will therefore look to allocating a sufficient budget for work in this area.

- Collective action: One of the most effective ways to deal with human rights issues is to work collectively with other companies, NGOs, law firms and experts to address effectively the human rights risks which are most serious and salient. This collaboration can provide a fresh perspective on human rights impacts and can demonstrate, often publically, a company’s commitment to human rights.

- Capacity building: Even though terminating a contract which is particularly problematic in terms of human rights impacts can sometimes seem like the easier option, it is generally a better investment for businesses to work with the relevant companies within their supply chains and value chains in order to improve their human rights standards.

- Potential defence: Effectively addressing potential human rights issues in supply chains can mitigate these risks and can serve as a defence if something does go wrong.

- Be proactive: The best way to protect yourself is to be proactive – prepare human rights specific training sessions, conduct human rights impact assessments and comprehensive human rights due diligence and put in place a human rights policy.

For more information and a detailed analysis by industry sector please see the full report available at human-rights-due-diligence.nortonrosefulbright.online.

For more information contact:

Robin Brooks
Partner, London
Tel +44 20 7444
robin.brooks@nortonrosefulbright.com

Milana Chamberlain
Partner, London
Tel +44 20 7444 3289
milana.chamberlain@nortonrosefulbright.com

Sam Eastwood
Head of business ethics and anti-corruption
Partner, London
Tel +44 20 7444 2694
sam.eastwood@nortonrosefulbright.com

Stuart Neely
Associate, London
Tel +44 20 7444 3289
stuart.neely@nortonrosefulbright.com

Gal Levin
Associate, London
Tel +44 20 7444 5034
gal.levin@nortonrosefulbright.com

Dan Jarman
Senior associate, London
Tel +44 20 7444 3619
dan.jarman@nortonrosefulbright.com

British Institute of International and Comparative Law

Professor Robert McCorquodale
Institute director
Tel +44 20 7862 5151
r.mccorquodale@biicl.org

Lise Smit
Research fellow in business and human rights
Tel +44 20 7862 5162
l.smit@biicl.org

A call for Collective Action

Collective Action is gaining attention as a powerful tool for businesses, NGOs and policymakers to fight corruption together.

The UK Anti-Corruption Summit, held in May 2016, was a valuable opportunity for Government Leaders actively to promote Collective Action, which directly addresses two key themes of the London Anti-Corruption Summit's agenda, namely

- The need collaboratively to improve the standards of various international anti-corruption efforts
- The need to engage stakeholders within society to promote these efforts.

Collective Action

Collective Action is a process of cooperation amongst various stakeholders, including businesses, governments and civil society. Fighting corruption collectively increases the impact and credibility of individual action. Common forms of anti-corruption Collective Action include anti-corruption declarations; integrity pacts; principle-based initiatives; and certifying business coalitions.

Businesses recognise that there are certain corruption issues which cannot be tackled alone. Collective Action provides opportunities for businesses, the public sector, and civil society to empower themselves through collaboration to develop new initiatives to tackle these systemic corruption issues. For example, in a tender process, Collective Action commitments like integrity pacts promote increased prospects of fair selection. For all stakeholders concerned, Collective Action contributes to enhanced public reputation and credibility.

At an international level, Collective Action can be used as a tool to help ensure the consistent and fair enforcement of regulations. National legislation and international conventions are further supplemented and bolstered by engaged industry stakeholders. If approached correctly, Collective Action can fill lacunae in legislation or augment inadequate local law.

Call to action

Collective Action efforts can be fostered internationally with renewed engagement from interested stakeholders (including most notably national governments) at a national and international level and increased publicity of the success of significant projects already underway, like initiatives within the extractive, shipping and energy industries.

In anticipation of the Summit, now is the time to think about what governments can do to engage in Collective Action in the wider business environment.

Challenges

- Does your government understand the potential impact of Collective Action?
- Is your government committed to supporting Collective Action?
- Is this commitment articulated in a formalised and published Anti-Corruption plan?
- Could your government engage more with businesses and NGOs in promoting and developing Collective Action initiatives?

Leaders should use the Summit as a key platform to support Collective Action and create opportunities for Collective Action initiatives. Furthermore, Government Leaders should recognise and promote Collective Action as a collaborative and innovative tool to address systemic and deep-rooted corruption.

A version of this article was included in the Leader's Anti-Corruption Manifesto published by Transparency International UK in advance of the Summit.

For more information contact:

Sam Eastwood
Head of business ethics and anti-corruption
Partner, London
Tel +44 20 7444 2694
sam.eastwood@nortonrosefulbright.com

Key contacts

Sam Eastwood
Head of business ethics and anti-corruption
London
Tel +44 20 7444 2694
sam.eastwood@nortonrosefulbright.com

Asia Pacific

Alfred Wu
Hong Kong
Tel +852 3405 2528
alfred.wu@nortonrosefulbright.com

Abigail McGregor
Sydney
Tel +61 408 833 490
abigail.mcgregor@nortonrosefulbright.com

Sun Hong
Shanghai
Tel +86 21 6137 7020
hong.sun@nortonrosefulbright.com

Wilson Ang
Singapore
Tel +65 6309 5392
wilson.ang@nortonrosefulbright.com

Canada

Sally Gomery
Ottawa
Tel +1 613 780 8604
sally.gomery@nortonrosefulbright.com

Richard Wagner
Ottawa
Tel +1 613 780 8632
richard.wagner@nortonrosefulbright.com

François Fontaine
Montréal
Tel +1 514 847 4413
francois.fontaine@nortonrosefulbright.com

Europe

Sam Eastwood
London
Tel +44 20 7444 2694
sam.eastwood@nortonrosefulbright.com

Lista M. Cannon
London
Tel +44 20 7444 5991
lista.cannon@nortonrosefulbright.com

Ep Hannema
Amsterdam
Tel +31 20 462 9413
ep.hannema@nortonrosefulbright.com

Jason Hungerford
London
Tel+44 20 7444 2474
jason.hungerford@nortonrosefulbright.com

Aydin Jebrailov
Moscow
Tel +7 499 924 5101
aydin.jebrailov@nortonrosefulbright.com

Christian Dargham
Paris
Tel +33 1 56 59 52 92
christian.dargham@nortonrosefulbright.com

Piotr Strawa
Warsaw
Tel +48 22 581 4994
piotr.strawa@nortonrosefulbright.com

Latin America

Glenn Faass
Rio de Janeiro
Tel +5521 97220 9314
glenn.faass@nortonrosefulbright.com

Andrew Haynes
Rio de Janeiro
Tel +5521 3616 6996
andrew.haynes@nortonrosefulbright.com

Mauricio Zagarra-Cayón
Bogotá
Tel +57 1 746 4601
mauricio.zagarra-cayon@nortonrosefulbright.com

Luis Ernesto Andueza
Caracas
Tel +58 212 276 0007
luis.andueza@nortonrosefulbright.com

Middle East

Patrick Bourke
Dubai
Tel +971 4 369 6305
patrick.bourke@nortonrosefulbright.com

Orlando Vidal
Dubai
Tel +971 4 369 6398
orlando.vidal@nortonrosefulbright.com

South Africa

Andre Vos
Johannesburg
Tel +27 11 685 8865
andre.vos@nortonrosefulbright.com

United States

Michael J. Edney
Washington, DC
Tel +1 202 662 0410
michael.edney@nortonrosefulbright.com

Kevin James Harnisch
Washington, DC
Tel +1 202 662 4520
kevin.harnisch@nortonrosefulbright.com

Global resources

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We employ 3500 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Our office locations

People worldwide

7000+

Legal staff worldwide

3500

Offices

50+

Key industry strengths

- Financial institutions
- Energy
- Infrastructure, mining and commodities
- Transport
- Technology and innovation
- Life sciences and healthcare

Europe

Amsterdam	Monaco
Athens	Moscow
Brussels	Munich
Frankfurt	Paris
Hamburg	Piraeus
London	Warsaw
Milan	

United States

Austin	New York
Dallas	St Louis
Denver	San Antonio
Houston	San Francisco
Los Angeles	Washington DC
Minneapolis	

Canada

Calgary	Québec
Montréal	Toronto
Ottawa	Vancouver

Latin America

- Bogotá
- Caracas
- Rio de Janeiro

Asia Pacific

- Bangkok
- Beijing
- Brisbane
- Hong Kong
- Jakarta[1]
- Melbourne
- Port Moresby (Papua New Guinea)
- Perth
- Shanghai
- Singapore
- Sydney
- Tokyo

Africa

- Bujumbura[3]
- Cape Town
- Casablanca
- Dar es Salaam
- Durban
- Harare[3]
- Johannesburg
- Kampala[3]
- Nairobi[3]

Middle East

- Abu Dhabi
- Bahrain
- Dubai
- Riyadh[2]

Central Asia

- Almaty

1 TNB & Partners in association with Norton Rose Fulbright Australia
2 Mohammed Al-Ghamdi Law Firm in association with Norton Rose Fulbright (Middle East) LLP
3 Alliances

NORTON ROSE FULBRIGHT

Norton Rose Fulbright

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 3500 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, Africa, the Middle East and Central Asia.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.