Global Investigations Review

The Guide to Monitorships

Editors
Anthony S Barkow, Neil M Barofsky and Thomas J Perrelli

The Guide to Monitorships

Editors:

Anthony S Barkow

Neil M Barofsky

Thomas J Perrelli

GIR

Global Investigations Review

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.globalinvestigationsreview.com

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as at April 2019, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to: natalie.clarke@lbresearch.com.
Enquiries concerning editorial content should be directed to the Publisher:
david.samuels@lbresearch.com

ISBN 978-1-83862-224-4

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

ALIXPARTNERS

BROWN RUDNICK LLP

CROWELL & MORING LLP

DEBEVOISE & PLIMPTON LLP

FORENSIC RISK ALLIANCE

FOX CORPORATION

GUIDEPOST SOLUTIONS LLC

JENNER & BLOCK LLP

KATTEN MUCHIN ROSENMAN LLP

KIRKLAND & ELLIS LLP

KOBRE & KIM

LALIVE SA

McKOOL SMITH

ROPES & GRAY INTERNATIONAL LLP

SIMPSON THACHER & BARTLETT LLP

UNIVERSITY OF IOWA COLLEGE OF LAW

VENABLE LLP

WILMER CUTLER PICKERING HALE AND DORR LLP

Publisher's Note

The Guide to Monitorships is published by Global Investigations Review – the online home for all those who specialise in investigating and resolving suspected corporate wrongdoing.

It aims to fill a gap in the literature – the need for an in-depth guide to every aspect of the institution known as the 'monitorship', an arrangement that can be challenging for all concerned: company, monitor and appointing government agency. This guide covers all the issues commonly raised, from all the key perspectives.

As such, it is a companion to GIR's larger reference work – *The Practitioner's Guide to Global Investigations* (now in its third edition), which walks readers through the issues raised, and the risks to consider, at every stage in the life cycle of a corporate investigation, from discovery to resolution.

We suggest that both books be part of your library: *The Practitioner's Guide* for the whole picture and *The Guide to Monitorships* as the close-up.

The Guide to Monitorships is supplied to all GIR subscribers as a benefit of their subscription. It is available to non-subscribers in online form only, at www.globalinvestigationsreview.com.

The Publisher would like to thank the editors of this guide for their energy and vision. We collectively welcome any comments or suggestions on how to improve it. Please write to us at insight@globalinvestigationsreview.com.

Preface

Corporate monitorships are an increasingly important tool in the arsenal of law enforcement authorities, and, given their widespread use, they appear to have staying power. This guide will help both the experienced and the uninitiated to understand this increasingly important area of legal practice. It is organised into five parts, each of which contains chapters on a particular theme, category or issue.

Part I offers an overview of monitorships. First, Neil M Barofsky – former Assistant US Attorney and Special Inspector General for the Troubled Asset Relief Program, who has served as an independent monitor and runs the monitorship practice at Jenner & Block LLP – and his co-authors Matthew D Cipolla and Erin R Schrantz of Jenner & Block LLP explain how a monitor can approach and remedy a broken corporate culture. They consider several critical questions, such as how can a monitor discover a broken culture? How can a monitor apply 'carrot and stick' and other approaches to address a culture of non-compliance? And what sorts of internal partnership and external pressures can be brought to bear? Next, former Associate Attorney General Tom Perrelli, independent monitor for Citigroup Inc and the Education Management Corporation, walks through the life cycle of a monitorship, including the process of formulating a monitorship agreement and engagement letter, developing a work plan, building a monitorship team, and creating and publishing interim and final reports.

Nicholas Goldin and Mark Stein of Simpson Thacher & Bartlett – both former prosecutors with extensive experience in conducting investigations across the globe – examine the unique challenges of monitorships arising under the Foreign Corrupt Practices Act (FCPA). FCPA monitorships, by their nature, involve US laws regulating conduct carried out abroad, and so Goldin and Stein examine the difficulties that may arise from this situation, including potential cultural differences that may affect the relationship between the monitor and the company. Additionally, Alex Lipman, a former federal prosecutor and branch chief in the Enforcement Division of the Securities and Exchange Commission (SEC), and Ashley Baynham, fellow partner at Brown Rudnick LLP, explore how monitorships are used in resolutions with the SEC. Further, Bart M Schwartz of Guidepost Solutions LLC – former Chief of the

Criminal Division in the Southern District of New York, who later served as independent monitor for General Motors – explores how enforcement agencies decide whether to appoint a monitor and how that monitor is selected. Schwartz provides an overview of different types of monitorships, the various agencies that have appointed monitors in the past, and the various considerations that go into the decisions to use and select a monitor.

Part II contains three chapters that offer experts' perspectives on monitorships: that of an academic, an in-house attorney and forensic accountants at Forensic Risk Alliance. Professor Mihailis E Diamantis of the University of Iowa provides an academic perspective, describing the unique criminal justice advantages and vulnerabilities of monitorships, as well as the implications that the appointment of a monitor could have for other types of criminal sanctions. Jeffrey A Taylor, a former US Attorney for the District of Columbia and chief compliance officer of General Motors, who is now executive vice president and chief litigation counsel of Fox Corporation, provides an in-house perspective, examining what issues a company must confront when faced with a monitor and suggesting strategies that corporations can follow to navigate a monitorship. Finally, Frances McLeod and her co-authors at Forensic Risk Alliance explore the role of forensic firms in monitorships, examining how these firms can use data analytics and transaction testing to identify relevant issues and risk in a monitored financial institution.

Part III includes four chapters that examine the issues that arise in the context of cross-border monitorships and the unique characteristics of monitorships in different areas of the world. First, litigator Shaun Wu, who served as a monitor to a large Chinese state-owed enterprise, and his co-authors at Kobre & Kim examine the treatment of monitorships in the East Asia region. Switzerland-based investigators Daniel Bühr and Simone Nadelhofer of Lalive SA explore the Swiss financial regulatory body's use of monitors. Judith Seddon, an experienced white-collar solicitor in the United Kingdom, and her co-authors at Ropes & Gray International LLP explore how UK monitorships differ from those in the United States. And Gil Soffer, former Associate Deputy Attorney General, former federal prosecutor and a principal drafter of the Morford Memo, and his co-authors at Katten Muchin Rosenman LLP consider the myriad issues that arise when a US regulator imposes a cross-border monitorship, examining issues of conflicting privacy and banking laws, the potential for culture clashes, and various other diplomatic and policy issues that corporations and monitors must face in an international context.

Part IV includes five chapters that provide subject-matter and sector-specific analyses of different kinds of monitorships. For example, with their co-authors at Wilmer Cutler Pickering Hale and Dorr LLP, former Deputy Attorney General David Ogden and former US Attorney for the District of Columbia Ron Machen, co-monitors in a DOJ-led healthcare fraud monitorship, explore the appointment of monitors in cases alleging violations of healthcare law. Günter Degitz and Richard Kando of AlixPartners, both former monitors in the financial services industry, examine the use of monitorships in that field. Along with his co-authors at Kirkland & Ellis LLP, former US District Court Judge, Deputy Attorney General and Acting Attorney General Mark Filip, who returned to private practice and represented BP in the aftermath of the Deepwater Horizon explosion and the company's subsequent monitorship, explores issues unique to environmental and energy monitorships. Glen McGorty, a former federal prosecutor who now serves as the monitor of the New York City District Council of Carpenters and related Taft-Hartley benefit funds, and Joanne Oleksyk of Crowell & Moring

LLP lend their perspectives to an examination of union monitorships. Michael J Bresnick of Venable LLP, who served as independent monitor of the residential mortgage-backed securities consumer relief settlement with Deutsche Bank AG, examines consumer-relief fund monitorships.

Finally, Part V contains tnwo chapters discussing key issues that arise in connection with monitorships. McKool Smith's Daniel W Levy, a former federal prosecutor who has been appointed to monitor an international financial institution, and Doreen Klein, a former New York County District Attorney, consider the complex issues of privilege and confidentiality surrounding monitorships. Among other things, Levy and Klein examine case law that balances the recognised interests in monitorship confidentiality against other considerations, such as the First Amendment. And former US District Court Judge John Gleeson, now of Debevoise & Plimpton LLP, provides incisive commentary on judicial scrutiny of DPAs and monitorships. Gleeson surveys the law surrounding DPAs and monitorships, including the role and authority of judges with respect to them, as well as separation-of-powers issues.

Acknowledgements

The editors gratefully acknowledge Jenner & Block LLP for its support of this publication, as well as Jessica Ring Amunson, co-chair of Jenner's appellate and Supreme Court practice, and Jenner associates Jessica Martinez, Ravi Ramanathan and Tessa JG Roberts for their important assistance.

Anthony S Barkow, Neil M Barofsky and Thomas J Perrelli
April 2019
New York and Washington, DC

Contents

Part III

International and Cross-Border Monitorships

12

US-Ordered Cross-Border Monitorships

Gil M Soffer, Nicola Bunick and Johnjerica Hodge[1]

A monitorship can be difficult to manage in the best of circumstances. Even the most basic arrangement requires the monitor to evaluate a company that he or she does not represent, report to an agency for which he or she does not work, and gather sensitive information without invading attorney–client privilege. Worse, the company will almost certainly not welcome the monitorship, let alone the intrusive features of it – including the monitor's examination of proprietary data, interviews of company personnel and customers, and findings that could require the company to abandon well-established practices or discipline long-standing employees.

A US-ordered cross-border monitorship poses all these challenges and more. To monitor a company with operations outside the United States, especially one with operations around the globe, is to contend with several if not dozens of disparate legal systems and business cultures. As a result, while the work that a monitor typically performs – such as conducting interviews, collecting data, and recommending discipline – can be accomplished with little difficulty in the United States, it may be sharply restricted in some countries. Moreover, practices or attitudes that are commonplace in one affiliate may be radically different in another affiliate of the same company.

In the face of these legal and practical challenges, the cross-border monitor would do well to consider a few key attributes of cross-border monitorships before proceeding. First, it is not the monitor's primary job to investigative misconduct. That is a basic tenet of almost any monitorship, but one that is not always well understood. Second, the monitor may not be able to visit every place a company does business – particularly when the company operates around the world – and consequently must devise ways to assess the company's compliance with that limitation in mind. Third, foreign privacy and labour laws may apply and must

1 Gil M Soffer is a partner, and Nicola Bunick and Johnjerica Hodge are associates at Katten Muchin Rosenman LLP.

carefully be considered, as they could impede the monitor's work (or worse). The same is true for foreign laws governing the imposition and publicising of employee discipline. Finally, while companies must implement a coherent global compliance programme, local variations will be appropriate and necessary to account for differences in local business culture and practice.

The role of the monitor

The monitor is not always an investigator

Infrequent in the United States, monitorships are entirely unknown in many parts of the world. The first challenge facing a cross-border monitor is, therefore, the most fundamental: clarifying the role of a monitor, and perhaps more importantly, what the monitor is not. As the Department of Justice's guidance on corporate monitorships makes clear, the monitor's 'primary responsibility is to assess and monitor a corporation's compliance with the terms of the agreement specifically designed to address and reduce the risk of recurrence of the corporation's misconduct[2] . . . [t]he 'monitor's mandate is not to investigate historical misconduct.'[3]

Clarity on this issue is important in any monitorship; only by understanding the purpose of their work can monitors design an appropriate work plan and discharge their mandate effectively. In a cross-border monitorship, clarity of purpose is crucial. Some countries prohibit or restrict corporate investigations of misconduct,[4] and in these jurisdictions, the consequences of overextending the monitor's role could be significant. If witnesses mistake the monitor for a criminal investigator, they may report the monitor to the local authorities. Those authorities, which may previously have been unaware of the monitorship,[5] could begin investigating the monitored entity or insist on exploring the contours of the monitorship with the monitor and the enforcement agency. At the very least, interference of this kind would unnecessarily complicate the monitorship and potentially delay the monitor's work.[6] Before beginning their work outside the United States, monitors must ensure that the company and its employees – particularly the witnesses they intend to interview – clearly understand the monitor's role.

2 Craig S Morford, US Department of Justice, 'Selection and Use of Monitors in Deferred Prosecution Agreements and Non-Prosecution Agreements with Corporations', at 2 (7 March 2008), https://www.justice.gov/sites/default/files/dag/legacy/2008/03/20/morford-useofmonitorsmemo-03072008.pdf.

3 id., at 6.

4 e.g., KPMG International, 'Cross-border investigations: Are you prepared for the challenge?', at 10 (2013), https://assets.kpmg/content/dam/kpmg/pdf/2013/12/cross-border-investigations.pdf. ('In some jurisdictions, it can be illegal for companies to investigate alleged employee misconduct because the local government considers itself to be the exclusive investigator responsible for law enforcement.')

5 In some countries, the monitor may be required to notify the local government or regulator if he or she is doing work there. Even where such disclosure is not required, it may still be considered good practice.

6 A similar risk exists in traditional internal investigations, where employees may 'seek the intervention of local government officials' in an attempt '[t]o deflect from the investigation.' John Frangos, 'Southeast Asia: Conducting Successful Corporate Internal Investigations', Society for Human Resource Management (28 August 2017), https://www.shrm.org/resourcesandtools/legal-and-compliance/employment-law/pages/southeast-asia-investigations.aspx.

The monitor cannot go everywhere

When a company has wide-ranging operations across the world, potentially spanning multiple business lines, the monitor's team may be unable to visit each location during the course of the monitorship – nor should they. The monitor's goal is not to assess every facet of compliance in every jurisdiction where the company does business, but rather the company's overall compliance environment. Accordingly, the monitor must think critically about which sites to visit, bearing several considerations in mind.

First, the monitor should make a priority of reviewing the company's operations in jurisdictions that pose the highest risk. These will almost certainly include locations where the underlying misconduct occurred. They may also include countries where the company's largest operations are situated, or where the highest-risk functions take place. Another indicator of risk is the nature of the violations that led to the monitorship in the first place. In cases involving Foreign Corrupt Practices Act (FCPA) violations, for example, the monitor should focus on countries with a known corruption risk – taking into account Transparency International's Corruption Perception Index[7] and any risk rankings generated by the company itself.

The more difficult choices arise beyond the highest-risk locations. Because monitors cannot go everywhere, they should identify a representative sample of locations that will enable them to assess the company's global compliance efforts, which can be a formidable task. Compliance risks can vary not only by country but by business line, business unit and even by product. They can also depend on the business model. Joint ventures, in which authority is shared between the monitored entity and its partner, may pose a greater risk than wholly owned subsidiaries, over which the company has full control. Manufacturing plants may be riskier than commercial operations, and commercial operations riskier than distributorships. Recent acquisitions typically pose an enhanced compliance risk, especially where the acquired company's compliance culture is immature and not yet fully integrated into the company's global culture.

How can a monitor assess the adequacy of a company's global compliance programme under these circumstances? One viable strategy is to identify common operational or other relevant features among the company's different affiliates; group the affiliates according to those common features; visit an affiliate within a group; and extrapolate findings from that affiliate to others in the same group. Deciding which common features to select depends heavily on the company at issue, of course, but the following are a few options:

- Common reporting structure: the monitor should consider whether business operations fall under the same global reporting structure. If several sites report up to the same business unit or managers, they will at least have some elements of supervision in common. Depending on the conduct under review, the monitor may be able to draw some conclusions about the adequacy of compliance by evaluating the common supervisory team.
- Common processes: if the company has compliance processes that vary from region to region or among different business lines, the monitor can group sites according to the processes they share. In an FCPA inquiry, for example, the company might employ the

7 Transparency International, Corruption Perceptions Index, Overview, https://www.transparency.org/research/cpi/overview (last visited 4 February 2019).

same third-party due diligence procedures at five of 25 affiliates. The monitor could test the procedures at one of the five affiliates, and extrapolate his or her findings to the remaining four in the same group (after accounting for any site-specific anomalies).

- Common business models: a monitored company might employ different business models across the world, each with a different risk profile. The monitor should test each model – especially those that present heightened risk, like recent acquisitions.
- Common systems: a key component of any functioning compliance programme is internal controls, which are usually embedded within a company's enterprise resource planning and procurement systems. If the company employs a unified global platform across all of its affiliates, the monitor's examination of internal controls may be relatively simple. But if the company does not make use of a single platform – as is often the case for companies that have expanded through acquisitions – there may be multiple legacy systems, each with its own user interface and technical challenges. In these cases, the monitor should endeavour to visit representative sites where each of the systems is in use.

All of these approaches can be fruitful under the right circumstances. But they are of limited value for assessing a company affiliate that does not share common features with any other, and where the monitor simply cannot visit because of civil unrest, armed conflict, public health emergencies, or the like. Such affiliates are a vexing challenge for the monitor – especially in corruption cases, where they are often located in the same countries that pose the highest corruption risk – and dealing with these locations requires some creative thinking. Among others, the monitor team could perform remote transaction testing, conduct video interviews with in-country employees, and interview in person any employees outside the country who may be assisting the affiliate with implementing financial and compliance controls.

Observing privacy and labour laws

Privacy

Companies in cross-border monitorships must abide by the privacy laws of the countries in which they operate. The complexity of these laws can be daunting for the monitored entity and the monitor alike, but they are vitally important to the cross-border monitor: because the life blood of a monitorship is information, any limitations on acquiring it could jeopardise the monitor's ability to fulfil his or her mandate. It is, therefore, incumbent on the monitor team to identify applicable privacy laws in advance of its work, and take the steps necessary to comply with them.

Among the most recent and best known privacy laws that monitors must contend with is the EU General Data Protection Regulation (GDPR). The GDPR restricts the ability of companies that operate, provide services, sell goods, or even track the behaviour of individuals[8] in the European Union and Member States from processing personal information without first

8 European Commission, 'Who does the data protection law apply to?', https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en (last visited 4 February 2019) ('The law applies to: 1. A company or entity which processes personal data as part of the activities of one of its branches established in the EU, regardless of where the data is processed; or 2. A company established outside the EU offering goods/services (paid or for free) or monitoring the behavior of individuals in the EU.')

obtaining permission to collect and distribute it, or satisfying one of several other specified criteria for processing the information.[9] Processing is defined broadly to include 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available'.[10]

Additionally, and perhaps most relevant to the activities of a monitor, the GDPR restricts companies from transferring personal data to countries lacking – in the eyes of the European Commission – adequate protection for personal data.[11] To satisfy the requirements of the GDPR, the monitor may need to enter into an agreement with the monitored entity to verify the steps the monitor will take to protect personal data being transferred by the monitored entity.[12] Further, depending on the monitorship, the monitor may hire third-party experts, accounting firms, data processing companies and others. The GDPR would govern the monitor's transfer of personal data from the monitored entity to any such third parties. As a result, the monitor may also need to enter into contractual arrangements with these vendors to ensure that the monitored entity can lawfully share information.

The monitor should also be aware that countries within the European Union are free to enact requirements that surpass those found within the GDPR. Thus, monitors must assess not only the GDPR, but any country-specific laws that may govern the transfer of information from the monitored entity to the monitor. And, of course, countries in the European Union are not alone in imposing privacy-related restrictions.[13]

In addition to restricting access to documents, privacy laws also address the manner in which the monitor and monitored entity receive reports of wrongdoing throughout the monitored entity.[14] Most multinational companies have established a reporting mechanism or 'hotline' through which employees can report potential misconduct either by company employees or by a third party associated with the company. Some countries permit companies to implement confidential-reporting systems, but others may require companies to

9 Regulation 2016/679 Of the European Parliament and of the Council of 27 April 2016, Article 6(1), GDPR, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN. The GDPR imposes even stricter requirements on the distribution of information related to criminal offences. See also id., Article 10.

10 GDPR, Article 4(2).

11 GDPR, Article 45(1) ('A transfer of personal data to a third country or an international organization may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection.')

12 See GDPR, Article 46(2)(f); see also id. Article 46(3) (noting that a third party can receive personal data if there are, among other things, 'contractual clauses between the controller or processor or the recipient of the personal data in the third country or international organization').

13 e.g., KPMG, Overview of China's Cybersecurity Law at 8, https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf (listing the privacy-related restrictions in China); see also Daniel Chen and Michael R Fahey, 'Data protection in Taiwan: overview', https://uk.practicallaw.thomsonreuters.com/5-578-3485?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1 (discussing the privacy-related restrictions in Taiwan).

14 e.g., Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN.

obtain permission from employees or government authorities before doing so.[15] Still other countries limit the types of conduct that can be reported, and others discourage any confidential reporting at all. [16]

In short, privacy laws can create stumbling blocks to the smooth transfer of information during the monitorship. The monitor and company must consider privacy issues as early as possible, and establish protocols for document and information transfers well in advance of the monitor's field work.

Labour

Local labour laws may also restrict the monitor's access to information, and to employees as well. Some countries in Europe, for example, require that employee representatives (known as work councils) must be consulted prior to an employee's interview.[17] In some countries, employees have the right to refuse to attend an interview or otherwise cooperate with the monitor. Employees in certain countries may also expect to receive, or at a minimum review, any notes taken during interviews or other materials prepared as a result of interviews.[18] Labour laws also limit the type of discipline companies can impose. Some labour laws impose penalties or other liabilities on companies for terminating an employee in a manner that does not comply with specified legal protections. Others restrict when employers can take disciplinary action against employees.[19] Such restrictions range from requiring an employer to impose discipline within a certain time frame to forcing an employer to follow a particular procedure before terminating an employee.[20]

There is, in short, great variety among the labour laws that companies and monitors may encounter. Sophisticated multinational companies are well aware of them. The monitor must thoroughly understand them as well, and can draw upon the company's own expertise for assistance. (The DOJ contemplates that very process, often requiring monitored companies

15 e.g., World Law Group, *Global Guide to Whistleblowing Programs,* 2016, 1, http://www.theworldlawgroup.com/wlg/Handbooks__Guides.asp (noting that, in Argentina, 'Companies must always notify their employees before the implementation of a whistleblower program'); See id. at 41(noting that 'the Czech Data Protection Authority has to be notified prior to the collecting or processing of personal data').

16 See id., at 62, 66, 69.

17 See e.g., Directive 2009/38/EC of the European Parliament and of the Council of 6 May 2009; see also Philipp von Holst, *Global Investigations Review: The European, Middle Eastern and African Investigations Review,* 2017 (25 May 2017), https://globalinvestigationsreview.com/benchmarking/the-european-middle-eastern-and-african-investigations-review-2017/1142027/germany ('[A] hostile works council can cause serious problems to an internal investigation from delaying it to blocking single measures and leaking information to the press').

18 See, KPMG International, 'Cross-border investigations: Are you prepared for the challenge?' at 17 ('Many countries have data privacy laws that allow a target or a witness to have access to certain investigatory material, including a written investigation report.')

19 See e.g., Juliana Sa de Miranda and Ricardo Caiado, 'Brazil: Handling Internal Investigations', *Global Investigations Review*: *The Investigations Review of the Americas,* (21 August 2018) https://globalinvestigationsreview.com/benchmarking/the-investigations-review-of-the-americas-2019/1173349/brazil-handling-internal-investigations ('As in many other Latin American countries, the Brazilian labour legislation is complex and inclined to protect employees. It is no overstatement that there is a culture of judicial claims by employees against employers in the country, even in cases of weak or lack of proper grounds').

20 See e.g., Donald C Dowling Jr, Lexology, Internal investigations in overseas workplaces, (2 April 2013), https://www.lexology.com/library/detail.aspx?g=8088dd7e-b170-43f4-a0ea-daf3fdfd2672.

to provide guidance to the monitor on applicable local law.) As with most aspects of the monitorship, careful planning is critical at the outset to account for and ensure compliance with local labour laws.

Publicising employee discipline

One of the monitor's most important tasks is to assess whether the monitored company has undertaken appropriate remedial measures in the wake of wrongdoing, and one of the most important of such measures is the disciplining of employees responsible for misconduct. Indeed, US regulators have repeatedly emphasised this component of a remediation programme. The Department of Justice Manual, for example, highlights appropriate discipline of employees as one of five components required for a company to demonstrate that it has timely and appropriately remediated FCPA violations. It also makes clear that discipline should extend not only to those who committed the misconduct, but also to those in oversight positions:

> *The following items will be required for a company to receive full credit for timely and appropriate remediation . . . Appropriate discipline of employees, including those identified by the company as responsible for the misconduct, either through direct participation or failure in oversight, as well as those with supervisory authority over the area in which the criminal conduct occurred.*[21]

The US Securities and Exchange Commission likewise emphasises appropriate discipline as a component of an effective compliance programme.[22]

Beyond underscoring the importance of discipline itself, the DOJ and SEC both encourage companies to turn discipline into a teaching opportunity. In describing how a company can effectively enforce its anti-corruption compliance programme, for example, those agencies have noted that '[m]any companies have found that publicizing disciplinary actions internally, where appropriate under local law, can have an important deterrent effect, demonstrating that unethical and unlawful actions have swift and sure consequences.'[23] The challenge for companies seeking to follow this guidance is discerning what, precisely, may or may not be 'appropriate under local law'.

The GDPR is a case in point. As noted, that law restricts the 'processing' of 'personal data'.[24] The regulation defines 'personal data' broadly to cover 'any information relating to an identified or identifiable natural person', the latter being any person 'who can be identified, directly or indirectly'.[25] This definition encompasses information that in the aggregate could be used to identify a particular person.[26] Likewise, 'processing' is defined broadly to include

21 2017 US Department of Justice Manual, Title 9-47.120(3)(c), available at https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977.

22 US Dep't of Justice & US Sec. & Exchange Comm'n, 'A Resource Guide to the U.S. Foreign Corrupt Practices Act' 59 (2012), https://www.sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf.

23 id.

24 GDPR, Article 6(1).

25 GDPR, Article 4(1).

26 Amelia Hairston-Porter, 'INSIGHT: EU Enacts New Data Privacy Regime with Potential Effects on Cross-Border Investigations', *Bloomberg Law* (28 September 2018), https://news.bloomberglaw.com/

the 'collection, recording, organization . . . storage . . . use . . . [or] dissemination' of personal data by either automated or non-automated means.[27] To the extent the GDPR applies to the dissemination of information about an incident of employee misconduct, a company would have to comply with the law's requirements before sharing any information. Among other steps, the company would be obliged to provide the employee with notice of how his or her data may be processed, and to conduct a legal analysis to assess whether the company has an appropriate legal basis to distribute the information.[28]

None of these data privacy protections should prohibit a company from publicising fully anonymised information about an incident of employee misconduct.[29] Nevertheless, companies operating in an environment of heightened sensitivity to employee privacy may be hesitant to engage in the legal analysis necessary to determine what information can be shared, and how, under local law. That is particularly true in countries where the privacy laws are new and the regulatory guidance sparse. Given the importance to US regulators of imposing and publicising appropriate discipline, however, monitors should be examining how companies make use of discipline – and companies should carefully consider what information they can share with employees.

Variations in local business culture and practices

Multinational companies must maintain a coherent global compliance programme, while at the same time contending with local distinctions in business culture and practice. That is no easy feat, especially for companies that span the globe, but the government and the monitor will expect nothing less. One key to success in this regard is understanding relevant local practices and adapting global compliance principles accordingly.

Corruption cases offer a useful illustration. Regardless of where a company operates, it can never, under the FCPA or other anti-bribery legislation, permissibly bribe a government official in exchange for business. The company's compliance policy must be unyielding on this point. But the means to prevent bribery from occurring may require some variation from country to country to account for the local business environment. In larger countries, for example, where the pool of qualified employees might be abundant, the company could, without jeopardising its business, choose not to hire any employee with close family ties to a distributor that sells company products to the government. In smaller countries, the relevant talent pool might be much smaller, making it impractical for the company to impose a blanket ban of this sort. Instead, the company might reasonably apply rigorous controls to its hiring process, like walling off potentially conflicted employees from any interactions with the distributor.

---

white-collar-and-criminal-law/insight-eu-enacts-new-data-privacy-regime-with-potential-effects-on-cross-border-investigations.

27 GDPR, Article 4(2).

28 GDPR permits companies to process personal data in a limited number of instances, including where the employee consents (although consent can be revoked), where necessary to comply with a legal obligation, and where necessary to pursue a legitimate company interest after this interest is balanced against the interests and rights of the employee. See GDPR Article 6(1)(a), (c), and (f) (lawfulness of processing) and GDPR Article 7(3) (consent may be withdrawn at any time).

29 Companies will need to consult with local experts on the full range of laws and regulations that may limit their ability to disseminate information about employee discipline in a particular jurisdiction.

The number of examples of this nature is nearly limitless. The point is that one size does not necessarily fit all in the implementation of a global compliance programme. Variations may be entirely appropriate and often critical. If a company's policies create significant practical barriers to conducting business in a particular country, the company runs a greater risk that employees will circumvent compliance controls. By calibrating its programme to account for local variations in business practice, while still maintaining a compliant environment, a company can make its compliance policies both more practical and more likely to be effective in the long run. Like the other lessons for cross-border monitors noted above – clarifying the monitor's role, strategically choosing the right locations to visit, and being mindful of privacy and labour laws – careful attention to local culture and practice will position the monitor well to achieve his or her primary mission: assessing whether the company's compliance programme adequately addresses and reduces the risks that led to the monitorship in the first place.

Appendix 1

About the Authors

Gil M Soffer
Katten Muchin Rosenman LLP

Gil M Soffer is managing partner of Katten's Chicago office, national co-chair of the firm's litigation practice and a member of the board of directors. A former federal prosecutor, Gil provides experienced counsel to individuals and companies under investigation by the Department of Justice (DOJ), Securities and Exchange Commission, Federal Trade Commission and other government regulators.

Gil's practice runs the gamut of white-collar criminal and civil fraud matters, with particular emphasis on the Foreign Corrupt Practices Act (FCPA), healthcare fraud, securities fraud and fraud involving government programmes. Gil has particular experience in the area of independent corporate monitorships. As Associate Deputy Attorney General, Gil was a principal drafter of the DOJ's Corporate Monitor Principles (the Morford Memo). He has testified before the US House of Representatives Judiciary Committee's Subcommittee on Commercial and Administrative Law regarding the use and selection of corporate monitors in criminal cases. In February 2017, the DOJ and SEC appointed Gil as the global corporate compliance monitor for the world's largest manufacturer of generic pharmaceuticals, in one of the most substantial FCPA resolutions to date.

Nicola Bunick
Katten Muchin Rosenman LLP

Nicola Bunick concentrates her practice on litigation and enforcement matters relating to the financial services industry, regulatory and internal investigations, and other complex commercial disputes. She has experience with federal litigation and has represented individuals and corporations in matters involving various government agencies.

Prior to joining Katten, Nicola served as senior counsel to US Senator Joe Donnelly. She also worked as an associate at a law firm in Washington, DC, focusing on antitrust matters, including government investigations, merger reviews and antitrust counselling.

Johnjerica Hodge
Katten Muchin Rosenman LLP

Johnjerica Hodge concentrates her practice on internal and government investigations, corporate compliance, environmental litigation and appellate litigation. She represents healthcare providers in investigations and related False Claims Act matters arising from allegations of Medicare and Medicaid fraud and abuse and violations of the Anti-Kickback Statute. Additionally, she provides counsel on billing and coding issues related to state laws. Johnjerica is a member of the independent compliance monitor team appointed in connection with a significant Foreign Corrupt Practices Act settlement by a pharmaceutical company, and she counsels clients on various environmental law, administrative law and constitutional law issues. Johnjerica has substantial experience in motion practice in state and federal courts and also devotes a portion of her practice to corporate compliance and business ethics issues.

Prior to joining Katten, Johnjerica served as a clerk for Chief Judge Carl E Stewart of the US Court of Appeals for the Fifth Circuit. During law school, she contributed to and was a member of the *Alabama Law Review*. She also interned in the Federal Tort Claims Act Litigation Section of the US Department of Justice and with the Honorable Lawrence S Coogler of the US District Court for the Northern District of Alabama.

Katten Muchin Rosenman LLP
525 W Monroe Street
Chicago, IL 60661
United States
Tel: +312 902 5200
nicola.bunick@kattenlaw.com
johnjerica.hodge@kattenlaw.com
gil.soffer@kattenlaw.com
www.kattenlaw.com

Since *WorldCom*, the United States Department of Justice and other agencies have imposed more than 80 monitorships on a variety of companies, including some of the world's best-known names.

The terms of these monitorships and the industries in which they have been employed vary widely. Yet many of the legal issues they raise are the same. To date, there has been no in-depth work that examines them.

GIR's *The Guide to Monitorships* fills that gap. Written by contributors with first-hand experience of working with or as monitors, it discusses all the key issues, from every stakeholder's perspective, making it an invaluable resource for anyone interested in understanding or practising in the area.

Visit globalinvestigationsreview.com
Follow @giralerts on Twitter
Find us on LinkedIn

ISBN 978-1-83862-224-4