GIR INSIGHT

EUROPE, THE MIDDLE EAST AND AFRICA INVESTIGATIONS REVIEW 2019

EUROPE, MIDDLE EAST AND AFRICA INVESTIGATIONS REVIEW 2019

Reproduced with permission from Law Business Research Ltd
This article was first published in June 2019
For further information please contact Natalie.Clarke@lbresearch.com

LAW BUSINESS RESEARCH

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

www.globalinvestigationsreview.com

To subscribe please contact subscriptions@globalinvestigationsreview.com

ISBN: 978-1-83862-226-8

Printed and distributed by Encompass Print Solutions
Tel: 0844 2480 112

Contents

Preface

Welcome to the *Europe, Middle East and Africa Investigations Review 2019*, a Global Investigations Review special report.

Global Investigations Review is the online home for all those who specialise in investigating and resolving suspected corporate wrongdoing, telling them all they need to know about everything that matters.

Throughout the year, the GIR editorial team delivers daily news, surveys and features; organises the liveliest events ('GIR Live'); and provides our readers with innovative tools and know-how products.

In addition, assisted by external contributors, we curate a range of comprehensive regional reviews – online and in print – that go deeper into developments than our journalistic output is able.

The *Europe, Middle East and Africa Investigations Review 2019*, which you are reading, is part of that series.

It contains insight and thought leadership from 28 pre-eminent practitioners from these regions.

Across 12 chapters, spanning around 120 pages, it provides an invaluable retrospective and primer. All contributors are vetted for their standing and knowledge before being invited to take part.

Together, these contributors capture and interpret the most substantial recent international investigations developments of the past year, with footnotes and relevant statistics. Other articles provide valuable background so that you can get up to speed quickly on the essentials of a particular topic.

This edition covers France, Germany, Nigeria, Switzerland and the UK from multiple angles; has overviews of money laundering, data transfer, the regulation of cryptocurrency and international cooperation between agencies; and discusses the value experienced forensic accountants will bring to most investigations.

Among the gems, it contains:

- A thorough review of data-protection provisions in all the regions covered by the book, including Africa and the Middle East.
- Similar tours d'horizons for anti-money laundering and the regulation of fintech.
- A chapter on Africa and the 'extra' stuff to bear in mind when investigating there, along with how to overcome challenges.
- A summary of a momentous year in France.
- A summary of a curious year in the UK, certainly for the Serious Fraud Office – and what to read into certain of its decisions and results.
- An analysis of the Financial Conduct Authority's year, and how it is using its investigatory powers in an inquisitorial fashion, plus how some target firms are now making strategic use of the partial settlement mechanism to hedge their bets.

Along the way, you will encounter a personal experiment in cryptocurrency by those authors; and learn how an accountant can be to an investigation what Jamie Martin, Sotheby's head of scientific research, is to detecting fake Rothkos.

Enjoy!

If you have any suggestions for future editions, or want to take part in this annual project, we would love to hear from you.

Please write to insight@globalarbitrationreview.com.

Global Investigations Review
London
May 2019

The Geopolitics of Data Transfer

Weng Yee Ng
Forensic Risk Alliance

Blocking statutes, banking secrecy and data protection are not new concepts, but now more than ever the challenges crystallising because of geopolitical shifts must be carefully assessed and responded to. We know all too well the life cycle of an investigation, with big ticket litigation frequently lasting years. Strategic decisions made at the outset of an investigation that only take into consideration the 'now', and do not extrapolate where future pitfalls may lie, can be very costly.

The past few years have seen significant developments in such data privacy regulation in Europe, the Middle East and Africa (EMEA). These have included the repeal of Safe Harbour and the introduction of the Privacy Shield, the EU General Data Protection Regulation (GDPR) coming into force in May 2018, the passing of the Data Privacy and Protection Law by the Qatari government, and the appointment of South Africa's first members of the Information Regulator to monitor and enforce provisions of the Protection of Personal Information Act (the POPI Act). It is fair to say that, with the advancement of and reliance on technology to conduct cross-border business, there will be no relaxation in data protection laws. Companies must be informed on how to navigate the ever-changing regulation, and cross-border, cross-jurisdictional data governance, transfer and protection challenges.

To add further uncertainty and complexity to the current regulatory environment, recent disruptive geopolitical developments, such as Brexit and the Trump administration's proposed approach to modernise US data privacy policy, will inevitably further highlight conflicts of law and add complexity to the issue of data transfers, especially in the context of investigations and disputes – and, by extension, e-discovery. Because regulatory investigations and related processes frequently span several years, strategic decisions made today around data transfers will have important ramifications down the line.

The existence and the robustness of established data protection laws globally varies significantly from one jurisdiction to another. In this article, we provide an overview of key data privacy regulations throughout EMEA, and set out some considerations and practical guidelines to minimise risk exposure for companies and professional services firms dealing with cross-border investigations and litigation.

Evolving privacy protection across EMEA: is it enough?

Europe

In 1995, the European Commission (EC) issued a Directive[1] that prohibited the transfer of personal data to non-EU countries that do not have an 'adequate' level of privacy protection. To bridge the differences in approach to data privacy and provide a mechanism to enable the free transfer of data between Europe and the United States, the US–EU Safe Harbour Framework (Safe Harbour) was developed, and has been in place for 15 years. Since then, with the increasing internationalisation of business and related data flows across borders, the EC recognised the lack of consistent safeguards around data privacy between member states and therefore proposed introducing true consistency through the GDPR. About a year after the EC began to draft the GDPR in 2012, Edward Snowden leaked information about the extent of the National Security Agency's mass surveillance and data collection practices, and almost concurrently an investigation into Facebook's European privacy practices was launched by the Irish data protection watchdog. In such an environment, it was almost inevitable that the European Court of Justice would review the 'adequacy' criteria of data protection in the United States. The results of that review led to the Safe Harbour Framework being invalidated in October 2015,[2] leaving corporates in a state of uncertainty around data protection and data transfer for months while an alternative mechanism was developed. The result was the development of the EU–US and Swiss–US Privacy Shield (the Shield), which, after much debate, eventually came into force in July 2016, with the intent of providing more accountability and oversight over data protection privacy. The initial reactions to earlier drafts of the Shield were sceptical. Max Schrems, the European privacy campaigner and lawyer who was instrumental in getting Safe Harbour struck down, tweeted: '#PrivacyShield: They put ten layers of lipstick on a pig but I doubt the Court & DPAs suddenly want to cuddle with it.'[3]

Despite its controversies, in October 2017, the EC's first annual review of the EU–US Privacy Shield found that, on the whole, the Privacy Shield 'continues to ensure an adequate level of data protection'. The EC, however, noted room for improvement and has provided recommendations for the functioning of the Shield that need to be taken on board by US authorities.

The GDPR was approved by the European Parliament in April 2016 and came into force on 25 May 2018, officially replacing the Data Protection Directive 95/46/EC (the Directive). The new regulation differs from the Directive on data privacy and data transfer in that the focus is now on accountability (as opposed to the old directive, which was based on notification requirements). This is clearly evidenced by the ongoing investigations and notices being served worldwide. Responsibility not only falls on a 'data controller' but also a 'data processor' – so eDiscovery consultants are held accountable as well. This means that the data controllers and data processors must implement technical and organisational measures, as well as demonstrate compliance when it comes to handling data that may cross multiple jurisdictions under the GDPR.

1 Data Protection Directive 95/46/EC.

2 Court Justice of the European Union 'The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid' Press Release No. 117/15.

3 Max Schrems (@maxschrems) 29 February 2016.

GDPR preserves the core principles and the Adequacy Criteria of the Directive, but aims to simplify the process for methods of cross-border transfer of data and aims to ensure security. There are many new obligations (some listed below) under the GDPR that require companies handling EU citizens' data to undertake major operational reform. One year after implementation, the potential for huge fines for GDPR non-compliance is being realised.

Codes of conduct

The GDPR endorses the use of codes of conduct and certifications to demonstrate compliance.

Expanded territorial reach

The territorial applicability under the GDPR is clear in that it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. Further, it applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, and non-EU businesses conducting processing activities of EU citizens will require the appointment of a representative within the EU.

Consent

The conditions for consent to process data have been strengthened and must be intelligible. A data subject's consent is required to be as easily withdrawn as it is granted.

International transfers risk awareness

Although the GDPR removes self-assessment as a basis for transfer, the consent derogation has undergone some changes. Data subjects are required to be adequately informed of the risk of transferring data outside the European Union.

Right to access

Individuals will have the right to access their personal data so that they are aware of and can verify the lawfulness of the data processing. The data controller must provide a copy of the personal data, free of charge.

Right to be forgotten

The right to be forgotten is the right for individuals to request the deletion or removal of personal data when there is no compelling reason for its continued processing.

Appointment of data protection officers

Currently, data controllers are required to notify local data protection authorities of any data processing activities. Under the GDPR, data protection officer appointment will be mandatory for controllers and processors whose core activities consist of processing operations.

Fines and penalties

Unlike previous regulations, the GDPR introduced a tiered penalty approach for breaches, where fines for breaches are much higher than under previous regulations (ie, up to 4 per cent of annual worldwide turnover or €20 million).

Based on these changes alone, it is clear that the GDPR will introduce significant undertakings and potential risks for all parties affected, from concerned subjects, to oversight bodies and corporations with a nexus to the European Union. The largest GDPR fine to date of €50 million was slapped on Google by the French Data Protection Authority (CNIL) in January 2019. According to CNIL, Google had breached the GDPR in two ways:

- by failing to meet transparency and information requirements; and
- by failing to obtain a legal basis for processing.

It begs the question of whether this sets the pattern of future penalties and fines as no other GDPR breach has seen a fine as large as Google's.

What about Brexit?

And then there is Brexit – threatening to leave the UK in a no man's land of data protection, potentially viewed by EU regulators as having a data protection environment that, like the US, does not provide sufficient protections. *The Independent* reported that Brexit will see '1,000 new laws passed unilaterally and without parliamentary scrutiny when European law is transposed into British law under the Great Repeal Bill'.[4] In June 2017, it was announced in the Queen's Speech that the Data Protection Bill (the Bill) will replace the Data Protection Act 1998 (the 1998 Act), setting new standards for protecting general data. The Bill introduces new powers and offences in relation to data protection while largely replicating existing powers under the 1998 Act, and increases the maximum level of fines in the United Kingdom so that it is consistent with the GDPR.

The third generation of this data protection law received royal assent on 23 May 2018 and its main provision commenced on 25 May 2018, enforceable by the Information Commissioner's Office. However, the UK's 2018 Data Protection Act closely resembles the GDPR, which means that there is unlikely to be significant impact changes to the law when the UK leaves the EU. For example, when Brexit does eventually happen, the UK will not have any assurances that data will be protected.[5]

To add to the complexity, there is also the issue of how to handle UK–US data transfer. The United Kingdom will have to demonstrate that it has protections in place with the United States that ensure the same level of protection as provided under the EU–US Privacy Shield. A potential solution for this is to use Switzerland as a model for the United Kingdom – it has an adequacy finding, meaning that it has a mirror of the Privacy Shield agreement with the United States. Thus, an agreement such as this would mitigate the potential to run afoul of EU regulations.

4 www.independent.co.uk/news/uk/politics/after-brexit-1000-new-laws-will-be-passed-with-no-parliamentary-scrutiny-a7656981.html.

5 www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.

Middle East

There are currently no pan-Middle Eastern or pan-Gulf Cooperation Council (GCC) laws governing data protection and privacy.

Israel is the only Middle Eastern country with data protection laws deemed adequate by the EC. Restrictions on transfer of data offshore are strict, and only include countries that ensure a level of protection of information that is not lower than the level of protection provided for under Israeli law.

Many Middle Eastern countries (GCC countries in particular) have also made considerable efforts to diversify their economies and increase economic integration in recent years. Saudi Arabia announced Vision 2030, which aims to increase the share of non-oil exports from 16 to 50 per cent over the next 15 years.[6] Other GCC countries have undertaken similar programmes, with the intent, like the UAE, to continue to attract international IT and finance companies and investment, and increase cross-border technology infrastructure. These developments imply the need to consider developing a data protection regime.

In international economic zones, such as in designated areas in the UAE and Qatar, data protection law, implementation and enforcement are relatively well developed. The Dubai International Financial Centre (DIFC) and the Qatar Financial Centre (QFC) have their own dedicated data protection laws and enforcement bodies mirroring best practices in the European Union. They all stipulate that personal data can only be transferred to an outside jurisdiction if an adequate level of protection for that personal data is ensured by laws and regulations that apply to the recipient, or if a special permit is approved by the regulatory bodies.[7,8] The DIFC also publishes a list of countries considered as being 'adequate' for this purpose, which notably excludes the United States. No such list exists for the QFC. That being said, these laws only apply to licensed entities operating in these special zones.

Further, the Abu Dhabi Global Market (ADGM), the international financial centre established in the UAE capital, issued a number of amendments in 2018 on the ADGM Data Protection Regulations 2015, which were enacted on 4 October 2015. The enhancements are designed to bring some of the definitions closer to international standards, provide clarity around the timing of certain obligations and expand the number of jurisdictions approved for the transfer of personal data. Some of the changes include recognition of the DIFC for data exports and an increase in the maximum fine, which will enhance the enforcement powers of the Office of Data Protection, an independent data protection regulator for the ADGM, which was established in December 2017.[9]

Nevertheless, to date, with the exception of Israel, no Middle Eastern or African countries are considered to have adequate data protection environments from an EU perspective. However, it

6 https://english.alarabiya.net/en/perspective/features/2016/04/26/Full-text-of-Saudi-Arabia-s-Vision-2030.html.

7 DIFC Law No. 1 of 2007 (Amended by Data Protection Law Amendment Law DIFC Law No. 5 of 2012), section 11, 12.

8 Qatar Financial Centre Legislation, Data Protection Rules, section 3.1, 3.2.

9 www.mondaq.com/x/671922/data+protection/Abu+Dhabi+Global+Market+updates+ADGM+Data+Protection+Regulations.

would appear that change is afoot: in 2016, Qatar became the first GCC member state to issue a generally applicable data protection law. The law, which came into effect in May 2017, poses a potential fine of 5 million Qatari riyals for non-compliance. While the law currently provides specific guidance on the transfer of personal data to other jurisdictions, we can expect that there will be further regulations issued to assist the current law's implementation.

In addition, there are general constitutional rights and sector-specific laws (notably in telecommunications, banking and medical information) related to data privacy in these countries. Depending on the circumstances, these laws may apply and should be considered when conducting international investigations or responding to litigation.

Given the geopolitical realities of the region, it is unlikely that any EU-type regime will be enacted in the Middle East in the near future. However, recent technological developments across the region suggest that authorities are quickly becoming aware of the challenges of international data privacy, which may have implications for the Middle East. In Saudi Arabia, there is a new freedom of information and protection of private data law under review by the Advisory 'Shura' Council.[10] Bahrain is the latest of the Gulf countries to introduce laws on data protection as it positions itself to be a data centre hub. The Personal Data Protection Law No. 30 of 2018 (PDPL) closely aligns to the EU GDPR bar three key differences: extraterritorial effect, creation of a new intermediary – the data protection supervisor, and a duty of due diligence on data managers.[11] The PDPL was published in July 2018 and will come into force on 1 August 2019. In Turkey, the Law on Protection of Personal Data No. 6698 was passed in 2016 and the Regulation on Deletion, Destruction and Anonymization of Personal Data was published in the Official Gazette No. 30224 in October 2017. In May 2017, the draft Regulation on Data Controller's Registry was submitted to public review and is soon expected to enter into force. Rapid regional economic transformation will also ensure that data privacy continues to be an important topic in the future.

Africa

Many African economies are becoming vibrant hubs of economic progress, but the pace in the data privacy development area has been considerably slower.

In June 2014, the African Union adopted the Convention on Cybersecurity and Personal Data Protection,[12] which many identified as a transformative moment for data protection in the region. However, to date, no country has undertaken its ratification, and the Convention requires 15 countries to ratify it before it enters into effect.

Morocco and Mauritius, both with robust data protection laws and active enforcement bodies, remain the notable exceptions in the continent, while the rest of the countries remain in their formative stages. Most countries include general constitution rights and sector-specific laws (notably in telecommunications) related to data privacy in Africa, but roughly half of the 54 countries on the continent still have no comprehensive data protection regulation and are not publicly working on adopting one. African countries with data protection laws have reported very

10 www.dlapiperdataprotection.com/?t=law&c=SA.

11 www.bna.com/insight-comprehensive-data-n73014482594/.

12 www.au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

few enforcement actions, and while most of the existing data protection laws hinge on the principle of adequacy, the same laws do not specify which countries are considered to be 'adequate'.

In Kenya, a data protection bill was expected to be presented in Parliament by the end of May 2014, but the bill had still not passed at the time of writing.[13] South Africa's POPI Act was signed into law in November 2013; however, no one knows when the POPI Act will become fully effective. At the end of Q1 2019, only a few of the sections have commenced, including the establishment of the Information Regulator, the empowerment of the Minister and the Information Regulator to make POPI Act Regulations and the procedure for regulations is now in place and POPI Regulations have been finalised.

Interestingly, the POPI Act might be one of the most stringent examples of data privacy initiatives. It prohibits the transfer of personal information outside South Africa, subject to certain exceptions; for example, where consent is provided and where the recipient is subject to a law or binding agreements that are able to demonstrate effectively data processing principles similar to the conditions for processing personal information under the POPI Act.[14] The POPI Act is also unique as it considers criminal penalties and imprisonment when convicted of a breach.[15]

Some key considerations

In EMEA, the approach to data protection varies significantly across the board, and we have seen how both developed economies and emerging markets suffer from regulatory disparity. Essentially, global convergence on the issue of data privacy remains unlikely. Some would argue that the European Union is pushing for the GDPR to be the 'gold standard' of data privacy for other countries to follow, while others would question costs associated with complying with these standards and suggest that protecting individuals' rights to this extent may be to the detriment of national security.

In Europe there are several factors dominating the political and data discourse, chief among them being Brexit and the new responsibilities related to the GDPR.

The first annual review of the Shield, published in October 2017, found that US authorities need to make improvements to ensure the successful functioning of the Shield. Recommendations included:

- the appointment of a permanent Privacy Shield Ombudsperson, as well as ensuring the empty posts are filled on the Privacy and Civil Liberties Oversight Board;
- closer cooperation between privacy enforcers, raising more awareness for EU individuals on how to exercise their rights under the Shield, notably how to lodge complaints; and
- more proactive and regular monitoring of companies' compliance with the Shield obligations by the US Department of Commerce.

13 www.itwebafrica.com/ict-and-governance/256-kenya/232836-kenyas-data-protection-bill-ready-for-adoption.

14 Protection of Personal Information Act of 2013, Chapter 9, section 72.

15 Protection of Personal Information Act of 2013, Chapter 11, section 107.

The review noted that over 2,400 companies have now been certified by the US Department of Commerce. Following from the report, the Commission will work with US authorities on the follow-up of its recommendations and will continue to closely monitor the functioning of the Shield, including US authorities' compliance with their commitments.

In Africa, the GDPR is expected to have an impact as its scope will also cover many data controllers and processors outside the European Union. This includes e-commerce websites or target advertising providers and their Africa-based processors, who will be directly subject to the new provisions. The free flow of data between European and African countries will therefore be conditional upon proactive law-making and an adequate level of data protection, equivalent to that set out by the GDPR. Therefore, a high standard of personal data protection compliance should be applied to ensure compliance with new regulations.

All these factors create uncertainty for companies operating across borders, and leave investors, management and stakeholders susceptible to uneasy regulatory transitions, high costs and exposure to the risk of heavy fines. For industry practitioners, and companies involved in investigations or expecting regulatory probes or even cross-border litigation, there is no single solution, but there are certain measures that can be undertaken in preparation to mitigate risks.

Data mapping

A clear data strategy is vital to any investigation where data may reside in several jurisdictions. Crucial considerations include knowing what data is being considered, the jurisdiction where the data resides, applicable data privacy regulations and what clearance is required, the origin of the data collection, and destinations of data transfer.

Depending on the nature and severity of the investigation, companies will be most successful if they take a conservative approach to data transfers, as privacy failures may (and most likely will) lead to sizeable liabilities. In addition, beyond the considerations listed above and the mechanisms potentially used for data transfer, from a strategic and practical perspective, it is worth acknowledging that once data is transferred into the United States it becomes 'discoverable' and little regard will be given to data protection rights that it may have attached in its country of origin.

Collection and preservation

Before carrying out a data collection or data preservation exercise, it must be ensured that the appropriate risk management tools have been engaged, and steps have been taken to ensure compliance with data privacy regulations in the jurisdiction the data is being hosted in. We counsel, in general, collection and preservation of data in its jurisdiction of origin.

Training and escalation

All personnel involved in investigations and data transfers should be provided with up-to-date training regarding data transfer protocols and jurisdictional data privacy regulations. They should also be trained to properly document the considerations and safeguards, throughout the investigation, for any data transfer. Escalation protocols should also be in place to ensure demonstrable consideration and consultation in relation to data transfer, especially for jurisdictions

with data privacy regulations that are more challenging to address. Identifying and engaging the appropriate counsel in each jurisdiction, as well as having data identification, processing and transfer experts with extensive cross-border experience in the European Union and elsewhere to assist internal stakeholders, is a necessity.

Data transfer strategy

A data transfer strategy taking into consideration the nature of the data, its origin, data privacy and other data-related constraints (banking secrecy, commercial and state secrecy, etc), and security should be developed in consultation with the company's advisers. The risks of using untested or controversial data transfer mechanisms should be weighed up and erring on the side of caution is advised. After all, it is not possible to close the stable door after the horse has bolted.

Legal and technical solutions

There are also legal and technical solutions available to companies to maintain data control during cross-border and cross-jurisdictional investigations and to help mitigate the risks. These include hosting data in-jurisdiction or using a mobile in-country solution; eliminating non-responsive, privileged, confidential or private materials; and redacting sensitive communications and cross-border duplication.

Expert advice

Finally, it is imperative to consult and involve expert data privacy and transfer experts, who are well versed in cross-border data privacy and transfer, in any cross-jurisdictional investigation, to help navigate the potential conflicts of law we have addressed in this article and to avoid considerable penalties. Strategic decisions regarding data made today in litigation or investigation may be subject to investigation and enforcement. From the data identification and location exercise, to the treatment of data in a manner compliant with applicable data privacy laws, to the mechanism employed, if appropriate, for data transfer, advice and execution by the right experts will be critical to success.

Weng Yee Ng
Forensic Risk Alliance

Weng Yee Ng is a director at Forensic Risk Alliance (FRA). She has over 16 years of experience in external and internal audit and forensic accounting. Her main experience includes: compliance reviews; internal investigations; litigation (both civil and criminal) support for multinational companies; risk assessments; evaluation of compliance programmes; procurement fraud matters; third-party due diligence; Foreign Corrupt Practices Act (FCPA) monitorships for both the DOJ and SEC; and disgorgement and penalty calculations.

Weng Yee is currently working on a risk assessment and evaluation of compliance programme for an aviation company. She has recently completed compliance monitorships for a medical devices company and for a financial transaction systems manufacturer, both with global presence, a proactive anti-bribery and corruption review for an international bank and several internal investigations into whistleblower alerts for a CAC 40 automotive original equipment manufacturer (OEM).

Having spent over six years working in-country in Malaysia, Weng Yee possesses a first-hand understanding of the business nuances and financial and reporting practices encountered in Malaysia and in other Southeast Asian countries. Prior to FRA, Weng Yee was involved in statutory audits, advising on initial public offering (IPO) and debt restructuring exercises, and performing SOX compliance audits for companies in, among others, the financial services, chemicals, construction, real estate, retail, pharmaceutical, education, electronics, extraction, oil and gas, and consumer goods sectors.

Weng Yee is multilingual in English, Malay, Cantonese and Mandarin, and is familiar with Bahasa Indonesia and Spanish. She has conducted work in the USA, Canada, Chile, Colombia, Costa Rica, Ireland, France, Germany, Switzerland, Hungary, Italy, South Africa, China, Indonesia, Philippines, Singapore, Thailand and Australia.

Weng Yee is recognised in *Who's Who Legal: Investigations* Forensic Accountants 2018 and 2019, which say: 'Weng Yee Ng stands out in the market for her extensive experience providing top-quality forensic accounting services for major corporations all over the world, with sources calling her extremely spot on, knowledgeable and efficient.'

FRA is a global market leader working with our clients to identify, analyse and mitigate the risks associated with international regulatory compliance obligations, litigation, internal and external multi-jurisdictional investigations. Unlike traditional accounting firms, we operate purely in the forensic space and generally have no conflicts. We have extensive cross-sector and cross-border experience and scalability anywhere in the world with globally integrated teams, having worked in more than 75 countries across both developed economies and emerging markets. As internationally recognised specialists in multi-jurisdictional investigations, we bring a high level of confidence to clients facing serious issues by providing clear, robust, and candid advice that is trusted by clients, regulators, courts and enforcement agencies. FRA leaders and team members include professionals with regulatory body and law enforcement agency experience including individuals who have worked for the UK Serious Fraud Office (SFO), US Securities and Exchange Commission (SEC), and US Federal Bureau of Investigation (FBI). We offer extensive data privacy and protection and jurisdiction-specific experience such as blocking statute, banking secrecy, commercial secrecy, global privacy legislation and security risks, state sponsored and other hacking, leaks, data loss and excessive data retention. Our expertise in complex data analytics, information technology, and data management lies at the core of our foundation. Our data analytics team seamlessly integrates with our forensic accounting, digital forensics, and eDiscovery teams to ensure an empirical approach to solving client problems and offers creative analytical and visualization solutions tailored to client needs. We build strong client relationships acting as partner, trusted adviser and thought leader. Many clients have relied on us for more than two decades to deliver client service excellence, subject matter expertise and global market knowledge. We take pride in our inclusive and diverse teams operating in our 'one firm' collaborative culture across disciplines and geographies with global mobility, many of whom are multinational and multilingual professionals. Our highly skilled and sophisticated leaders and team members are forensic accountants, former investment bankers, financial and data analysts, legal and litigation support professionals, database architects, electronic discovery and collection experts, software engineers, and certified computer examiners. We are recognised in industry listings, including *Who's Who Legal*, where our leaders and team members are referred to as 'first-rate in multi-jurisdictional investigations and government enforcement matters'.

Audrey House
16–20 Ely Place
London, EC1N 6SN
United Kingdom
Tel: +44 20 7831 9110

www.forensicrisk.com

Weng Yee Ng
wng@forensicrisk.com

As well as daily news, GIR curates a range of comprehensive regional reviews. This volume, the *Europe, Middle East and Africa Investigations Review 2019*, contains insight and thought leadership from 28 pre-eminent practitioners from these regions. Inside you will find chapters on France, Germany, Nigeria, Switzerland and the UK (from multiple angles); comparative pieces on money laundering, data transfer, the regulation of cryptocurrency and international cooperation between agencies; plus a guide to the challenges of investigating in Africa – and lots more.

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

ISBN 978-1-83862-226-8