GIR INSIGHT

EUROPE, MIDDLE EAST AND AFRICA INVESTIGATIONS REVIEW 2020

EUROPE, MIDDLE EAST AND AFRICA

INVESTIGATIONS REVIEW 2020

Reproduced with permission from Law Business Research Ltd
This article was first published in June 2020
For further information please contact Natalie.Clarke@lbresearch.com

Published in the United Kingdom
by Global Investigations Review
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL

www.globalinvestigationsreview.com

To subscribe please contact subscriptions@globalinvestigationsreview.com

ISBN: 978-1-83862-269-5

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

Contents

Preface

Welcome to the *Europe, Middle East and Africa Investigations Review 2020*, 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 2020*, which you are reading, is part of that series. It contains insight and thought leadership, from 32 pre-eminent practitioners from these regions.

Across 11 chapters, spanning around 150 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 chapters provide valuable background so you can get up to speed quickly on the essentials of a particular topic.

This edition covers France, Germany, Italy, Nigeria, Romania, Russia, Switzerland and the UK from multiple angles; has overviews on trends in anti-money laundering, and how to remediate, to use the parlance, issues inside African business.

Among the gems, it contains:

- a timeline of warnings missed by Danske Bank and other case studies from the fight against money laundering;
- one our best-ever pieces on investigating in Africa – and in particular the extra hurdles faced by anyone seeking to remediate how it operates in the continent;

- all the latest developments from France – where the blocking statute is again on the agenda and a new enforcer has tentatively bared its teeth;
- handy roadmaps for setting up investigations in Germany and Switzerland; and
- how Russia wants to go straight, and the SFO and the FCA's respective years – how successful were they? The verdict appears mixed.

And much, much more. We hope you enjoy the volume. 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@globalinvestigationsreview.com.

Global Investigations Review
London
May 2020

Russia: Key Issues as to Compliance Programmes and their Enforcement – an Update

Paul Melling, Roman Butenko, Ekaterina Kobrin and Oleg Tkachenko
Baker McKenzie

In summary

In recent years Russia has joined the mainstream in terms of its legislative attack on corruption and bribery in the business sector and in its efforts to both educate its business community on best practices when it comes to anti-corruption and to oversee and enforce anti-corruption measures. Without minimising the scale of the problem that Russia faces in achieving these objectives, this chapter provides an overview of recent anti-bribery and corruption legislative measures and the guidance provided to the Russian business community with regard to said measures and their enforcement.

Discussion points

- New anti-corruption legislation provides for corporate as well as individual liability for bribery in both the public and private sector
- Extensive official guidance from the Ministry of Labour as to how best to build a compliance infrastructure within your organisation and how best to monitor its effectiveness
- Materials posted online by the enforcement authorities support the task of providing compliance training to both your employees and those of your third-party service provider
- Obstacles to effective and efficient internal investigations, including strict personal data protection legislation rigidly applied and limitations on attorney–client privilege
- New opportunities for self-reporting but benefits of self-reporting still open to question

Referenced in this article

- Law on Combatting Corruption
- Law on Advocates' Activities and the Advocates' Community

The 15 months prior to the onset of the covid-19 crisis saw unprecedented official guidance from regulators across the globe on corporate compliance programmes. This guidance ranged from the US Department of Justice Criminal Division's Evaluation of Corporate Compliance Programs released in early 2019 and the recent French Compliance Function Guide, to the updated guidance on Evaluating Compliance Programmes, published in the UK in January 2020. Following several large cases involving cooperation between the National Financial Prosecutor's Office, the French Anti-Corruption Agency and UK Serious Fraud Office, the regulators in the UK (2019 Corporate Co-operation Guidance) and France (Guidelines on the Implementation of the Convention Judicial Public Interest Agreement) issued very helpful guides on cooperation with the authorities, which sets out regulators' expectations as to data retention and investigation efforts.

Russian authorities have also been busy providing practitioners with insight into the government's expectations for anticorruption compliance programmes. For the most part, the available guidance on building a compliance programme is consistent with international precedent, although there is still little insight specifically into the conduct of internal investigations and ensuring the possibility to retain and furnish evidence, including e-data. What one can say specifically is that, when rolling out a compliance programme in Russia, appropriate provisions in employment contracts and internal HR procedures will be of paramount importance. With that in mind, The Russian Ministry of Labour and Social Security (the Ministry of Labour, the employment regulator) and the standards communicated by it play a key role in the compliance process.

Legislation

Russia introduced an explicit requirement for companies to implement compliance measures in 2012.[1] The law sets out a very basic list of measures that served as an example of the minimum a company should consider implementing to comply with the requirement. This list is non-exhaustive and includes:

- introduction of a designated anti-corruption function;
- cooperation with the authorities;
- rolling out policies and procedures to ensure a good-faith operation;
- issue of a code of ethics and business conduct;
- prevention and resolution of conflicts of interest; and
- preventing unofficial reporting and the use of forged documents.

There are no specific standards set by law, even for these measures.

There is also no liability specified for failure to comply with these requirements: the Prosecutor's Office has been making modest efforts to enforce them by issuing written binding orders to comply with the requirements following an inspection. Non-compliance with such orders can then entail serious consequences, including a potential criminal liability for individual members of management who were responsible yet failed to act.

1 Russian Federal Law No. 273-FZ of 25 December 2008 'On Combating Corruption', Article 13.3 introduced 3 December 2012.

Having a set of compliance measures is intended to have a tangible effect on a company's liability for corruption. Companies can be held liable under the Code of Administrative Offences for undue payments made on their behalf or in their interests[2] and for the illegal employment of former government and municipal officials,[3] unless they have taken all possible measures to prevent the offence (corporate guilt).[4] Enforcement practice is not consistent: while in some cases companies were able to successfully plead that their anti-corruption compliance measures were sufficient, in a large number of cases the courts have hardly conducted (if at all) any analysis of the company's measures and whether they could serve as a condition for releasing the company from liability.

Elements of compliance: Russian Ministry of Labour practical guidance

The Ministry of Labour is the authority responsible for:

> *development and implementation and advisory/methodological support of measures aimed at preventing corruption in organizations, monitoring the implementation of these measures, and methodological support of such measures.*[5]

In this capacity, the Ministry of Labour has issued practical guidelines and recommendations concerning measures to prevent corruption in Russia and it has been very active in fulfilling this function. Since 2014, it has issued a large number of such guidelines and recommendations and we will review the most significant of these below.

State organisations and state companies in Russia for the most part roll out their anticorruption compliance programmes following these guidelines and recommendations and many privately held companies also rely on them. Although the documents issued by the Ministry of Labour are non-binding recommendations, they serve as benchmarks for the Prosecutor's Office and courts.

The guidelines and the early recommendations were issued in an environment in which anticorruption compliance was still very new in Russia and thus contain a considerable amount of tutorial material on overseas and international anticorruption regulations, best practice summaries and sample documents.

The guidelines were issued in Russian and we are not aware of any reliable translation.

2 Article 19.28 Russian Code of Administrative Offences. Only individuals can be penalised for criminal offences in Russia; companies are liable for the 'administrative offence' of corrupt payments, a concept similar to the crime of corporate corruption.

3 Article 19.29 Russian Code of Administrative Offences.

4 Article 2.1 Russian Code of Administrative Offences.

5 Decree No. 610 of the Russian Government of June 19, 2012 (as amended) 'On the Approval of the Regulations on the Ministry of Labour and Social Security of the Russian Federation'.

Anti-corruption compliance system

The document, entitled Guidelines for the Development and Adoption by Organizations of Measures to Prevent and Combat Corruption,[6] was central to the first set of guides passed by the Ministry of Labour in early 2015. It included the ministry's insight into what reasonable compliance measures should look like. The guide was last updated in 2018. In October 2019, the ministry issued another set of guidelines called Measures to Prevent Corruption in Organizations[7], which largely reiterates the same provisions but is more detailed and better organised. In line with globally evolving best practices, the more recent recommendations have more of a focus on anti-corruption risk assessment and third-party risk management.

According to the recommendations, the minimum set of compliance policies for a company includes an anti-corruption policy, a code of ethics and a code of business conduct. Other important areas to be covered by a company's normative acts are anti-corruption risk assessment, conflicts of interest, communication and training, internal monitoring and control, and management of third parties (eg, due diligence review, avoiding conflicts of interest, anti-corruption clauses).

The principles that, according to the ministry, the anti-corruption policies of a company should rest on do not come as a surprise to experienced practitioners. They are:

- tone from the top;
- communication of anti-corruption regulations to employees and their involvement in anti-corruption procedures;
- effective compliance;
- adequate assessment of risks;
- communication of expected compliance standards to business partners;
- liability and inevitable punishment for employees irrespective of their position; and
- regular internal monitoring and control.

The guidelines describe what an anti-corruption programme might look like, offer a sample set of measures and outline the process for the introduction and renewal of compliance programmes.

Organising a compliance function is an area in which management enjoys broad discretion. Companies are offered a lot of freedom as to how they want to structure their compliance function and what department will be responsible for compliance. Importantly, the compliance unit must have a direct reporting line to top management (but the document is silent as to reporting thereafter), should be sufficiently staffed and should be given the resources and powers to exercise its functions.

The guidelines, in their first edition in 2015, introduced the requirement for companies to conduct anti-corruption compliance risk assessment and they outlined very broadly procedures for risk assessment and associated record keeping. In 2019, risk assessment procedures were addressed specifically by the Ministry of Labour in a special set of recommendations.

6 https://rosmintrud.ru/ministry/programms/anticorruption/015/0.

7 https://rosmintrud.ru/uploads/magic/ru-RU/Ministry-0-106-src-1568817692.8748.pdf.

Dealing with conflicts of interest and enforcing the relevant policies and procedures is central to effective compliance and the ministry devotes a large part of the document to explaining the general and more industry specific rules (eg, detailing the risks for the financial sector or medical and pharmaceutical companies).

The expected standard of cooperation with the authorities includes a number of commitments, including:

- reporting corruption;
- non-retaliation against reporters (Russian legislation on this remains however pending);
- cooperation with investigators and inspectors; and
- retention of evidence.

Companies are recommended to participate in nationwide anti-corruption initiatives, such as, for example, the Anti-Corruption Charter of Russian Business.[8]

Anti-corruption risk assessment guidelines

One of the most recent guidelines was released by the Ministry of Labour in September 2019 and entitled Recommendations on the Procedure for Assessing Corruption Risks in an Organization.[9] The 25-page document is essentially a very detailed guide to what anti-corruption risk assessments should be. It also encloses sample documents introduced by companies in Russia, such as a risk assessment plan, a risk modelling report and a comprehensive risks map.

Earlier, in 2017, the ministry had already taken steps to issue recommendations for anti-corruption risk assessments, but the 2017 guide applied to state authorities and state corporations or companies only.[10] The new set of recommendations is offered to all entities.

When working on the 2019 risk assessment guide, the ministry apparently did extensive research into international best practice and widely accepted standards of anti-corruption risk assessment.

In our view, the document provides very good guidance, although, in our practice of advising clients in Russia on compliance risk assessment, we seldom come across procedures and records anywhere near so detailed and sophisticated.

The guidelines are organised as a step-by-step procedure for the identification, analysis and ranking of corruption risks. They consistently promote the idea of adequacy of risk assessment procedures for the specific company into which they are to be introduced, for example based on its size, industry sector and available resources. The basic recommendation is to start with a calendar plan, first identify the priority areas and then progressively roll out risk management procedures to all other aspects of the company's activities. This is a very reasonable recommendation and clients could benefit from taking it on board. Instead of waiting for the right moment to conduct a comprehensive risk assessment of all of the business, it makes sense to prioritise and start with the high risk areas.

8 http://against-corruption.ru/en/.

9 https://rosmintrud.ru/uploads/magic/ru-RU/Ministry-0-106-src-1568817604.7941.pdf.

10 https://rosmintrud.ru/ministry/programms/anticorruption/9/8.

In identifying high risk areas, companies are predictably invited to follow value-based and risk-based approaches. Government-facing functions are a priority, including sales via state procurement, obtaining licences, permits and approvals, and dealings with state officials in the course of inspections. Examples of other high risk areas listed by the ministry include procurement for company needs, real estate transactions, disposing of property including non-core assets, budgetary functions (providing loans, marketing, sponsorship), use of intermediaries and remuneration or bonus schemes for employees. Companies are reminded that compliance risks can be created not only by their own employees, but also by third parties (agents, consultants, distributors, among others).

When assessing risks, companies are expressly advised to take into account their exposure to the laws of other countries where they (or their business partners) operate, including the Foreign Corrupt Practices Act (FCPA) and UK Bribery Act.

The standard set by the ministry for risk assessment procedures includes collection of data through document review and interviews with key employees, risk modelling, identification of existing risks and controls and their owners, risk ranking, gap analysis and identification of remedial risk mitigation actions.

Employees' obligations and motivation

In October 2019, the Ministry of Labour published its Memorandum on Employee Duties and Motivation in Organizations.[11]

The ministry explained that the obligation to comply with anti-corruption policies and procedures should be made part of the employment contract and that disciplinary (employment law) sanctions should be consistently applied to employees who fail to meet those obligations.

In addition to the inevitable sanctions for those in breach of their employment contracts, companies are encouraged to introduce monetary and non-monetary benefits as motivation for compliance on the part of their employees. Companies should not discourage employee compliance by setting key performance indicators that lead employees to prioritise performance over compliance.

As everyone with experience in this market is well aware, it is very difficult to sanction employees and especially to terminate their contracts for corruption-related offences in the absence of a valid court verdict against the non-compliant employees. It remains to be seen if enforcement practice will move in the direction of giving companies more opportunity to sanction rogue employees. Recently our firm won several cases in Russia for clients arising from the termination of the contracts of employees who, according to internal investigations, had failed to comply with internal compliance policies and procedures. Nonetheless, the dominant practice for parting company with the non-compliant employee remains the mutually agreed separation agreement, often coupled with a monetary sum paid to the employee.

11 https://rosmintrud.ru/uploads/magic/ru-RU/Ministry-0-106-src-1568817742.8173.pdf.

Compliance function structure

The Ministry of Labour updated its model job description for the compliance role in 2018.[12] Formally, the guidelines applies to state corporations and state-owned entities, however private businesses can benefit from this example.

The document sets a ratio of 1 to 100 as a recommendation for the size of the compliance unit relative to the overall number of employees. In our experience, this is a very generous ratio that is seldom met in the headcount of compliance units in private clients.

As we note in more detail below, internal investigations remain a relatively unregulated area in Russia. The compliance function guidelines explain, however, that compliance officers should have a right to conduct internal checks, including interviewing employees, subject to this function being included within the scope of their functions by internal regulations.

Prosecutor's Office guidance

The Prosecutor's Office (together with its territorial subdivisions) is the main driver of enforcement practice for corporate corruption offences, as it is the authority in Russia that investigates corporate corruption cases under article 19.28 of the Russian Code of Administrative Offences.

Prosecutors also perform the function of overseeing compliance with anti-corruption laws as per the international treaty obligations of the Russian Federation. Designated anti-corruption compliance departments have been established at all levels of the Prosecutor's Office. As part of this function, they make inquiries into the existence of corporate compliance programmes. Prosecutors are frequent speakers at compliance conferences and roundtables.

The anti-corruption compliance department of the Prosecutor's Office on its designated website[13] publishes a wide range of educational materials that compliance managers may find helpful in their work, especially if they have limited resources. Local companies with international best practice support from global headquarters can also benefit from these materials. Particularly worthy of mention are the Prosecutor's memoranda on Corporate Liability for Corruption[14] and Gifts to Public Officials.[15]

The Prosecutor's website even hosts movies with role-played high-risk situations and these fit very well into internal compliance training programmes.

Internal investigations

The ability to conduct effectively internal investigations into corruption and related allegations is a hugely important element of an effective compliance programme, but this aspect of the work of compliance managers and counsel remains a blank area in the Russian regulatory framework: there is almost no official guidance or reliable enforcement practice. Practitioners often have to rely on their own interpretation of local laws and follow international best practice. This makes

12 https://rosmintrud.ru/ministry/programms/anticorruption/015/1.

13 https://genproc.gov.ru/anticor.

14 https://genproc.gov.ru/upload/iblock/dbc/yurlica_2019.pdf.

15 https://genproc.gov.ru/upload/iblock/577/anticor_zapret.pdf.

internal procedures (eg, investigation policies, rules on the use of corporate devices and IT systems, use of the company's property for private purposes) key to the process and companies should properly issue them as local normative acts.

The most problematic aspects of internal investigations include the treatment of personal data, correspondence and private information collected during the investigation, protection of attorney–client communications and work products and reporting internal findings to the authorities.

Personal data, correspondence and private information

The Russian Law on Protection of Personal Data and legislative requirements for the localisation of individuals' data in Russia has set the bar very high in protecting privacy in any internal investigation conducted in Russia.

In the absence of any official clarifications or court practice, the safest option to comply with the data privacy requirements is to seek written consent from all those being interviewed to any transfer of that person's personal data (even to associated companies in the same corporate group). Two options are possible:

- consent can be obtained in advance of any investigation being required, but should clearly state the purpose (ie. verification of correspondence to internal company policies and procedures); or
- specific consent can be obtained from the data owners at the beginning of the investigation.

If for any reason it is not possible to obtain consent, the investigating entities may invoke other legal grounds for personal data processing that do not require the employees' consent. For example, as the ultimate goal of internal anti-corruption investigations is to eliminate non-compliance with legislation and (probably) local internal policies, the processing of data of employees within the investigation can based on such legal grounds as:

- the necessity to achieve the objectives set out in Russian legislation; or
- the necessity to exercise the rights and legitimate interests of the operator or third parties.

Although this approach seems logical and is based on the law, we are not aware of any positive enforcement practice using this interpretation.

Properly documenting the investigation is essential. Companies should officially initiate the investigation with an order of the general director appointing individual investigators as the authorised representatives of the employer. In this case, the investigators will have access to the employees' data on behalf of the employer even without the written consent of the employees. Such an investigation would have to be completed within strict deadlines and would end with another order of the general director reporting the findings.

Internal investigations do not usually target information about an employee's private life, but today's working environment makes it impossible to draw a clear dividing line between one's private and professional life, especially for those who work with 24/7 availability. Hence, it is commonplace for employees to store some pieces of information about their private life

(eg, private photos, documents, correspondence) on their corporate devices. This information, if accidentally found, should be ignored and not used in the investigation. Search terms should be carefully formulated so as to minimise the risk of encountering this information.

There is criminal liability in Russia for the illegal collection or distribution of data about an individual's private life containing a personal or family secret without his or her consent, although a criminal prosecution for truly unintended collection of information as to an individual's personal life could not be justified. An appropriate internal policy on use of corporate IT solely for business purposes can be helpful in supporting a position that all information found on corporate IT must be business-related or in supporting an argument that by placing such information on corporate IT the employee has de facto consented to it being accessed.

Protection of attorney–client communications and work product

It is common knowledge that the Russian legal system has a different approach to the concept of legal privilege as compared to common law jurisdictions.

In Russia, irrespective of the area of law, legal advice and representation in court proceedings may be provided by advocates (practitioners who are the members of a Bar) and by other legal practitioners persons with few limitations.[16] However, professional secrecy is protected only in relationships between clients and advocates.

Article 9 of the Federal Law on Advocates' Activities and the Advocates' Community defines an advocate's secret very broadly: any information related to the provision by the advocate of legal services to his or her client.

This article also provides three types of guarantee against disclosure of this sensitive information:

- prohibition on calling and questioning advocates as witnesses concerning matters known to them in relation to their legal services;
- prohibition on searching advocates' premises except on the basis of a court order; and
- prohibition on using materials contained in the advocate's file (called a dossier) as evidence for prosecution of the advocate's clients.

In addition to the above, the Russian Criminal Procedural Code provides additional guarantees to protect advocates from pressure from the law-enforcement authorities. In particular, it establishes a special and complex procedure for initiating criminal cases against advocates. A decision as to the initiation of a criminal case against an advocate must be taken by the Regional Head of the Investigative Committee.[17] Mandatory escalation of the matter to this high level is aimed at decreasing the risk that low-level officers put pressure on the advocate by commencing an arbitrary criminal case against him or her.

16 Eg, generally practitioners who are not members of a Bar cannot act as defence attorneys in Russian criminal proceedings.

17 Article 448, sub-clause 1.10 Russian Criminal Procedural Code.

In post-Soviet Russia, the Russian Constitutional Court in a number of cases[18] stressed that advocates enjoy special protection from search and seizure.

Some cases have been escalated to the European Court of Human Rights (ECHR), where legal advisers other than advocates have been seeking similar treatment. In the most recent and important case against Russia (*Kruglov and others v Russia*),[19] the court stated that it would be incompatible with the rule of law to leave without any particular safeguards to the relationship between clients and their legal advisers who, with few limitations, practise, professionally and often independently, in most areas of law, including representation of litigants before the courts. Given this, the court found that searches without judicial authorisation of the premises of the applicants in that case, who were practising lawyers but not advocates, had been conducted arbitrarily.[20] The ECHR underlined that those practitioners who do not have advocate status should therefore enjoy the same safeguards as to the protection of privileged documents and information as advocates possess.

It remains to be seen how this ECHR opinion will affect Russian practice. Thus far, Russian law has not been amended. It still provides protection for privileged information only to those legal professionals who are advocates. We believe that unless and until privilege protection is introduced as a new law, any documents and information seized from the premises of those professionals who are not advocates would be admissible evidence in Russian courts.

Even the participation of advocates in an investigation is not an absolute guarantee against disclosure of their privileged documents. Cases of attorney–client privilege violation by Russian law enforcement authorities are still reported even where advocates are involved. However, the community of advocates vigorously defends its members and their exclusive rights provided by the law – with cases of violation receiving massive press coverage and having decreased substantially over recent years. All these efforts have had a positive effect on law enforcement practice and have resulted in a more cautious approach by the law enforcement authorities towards violating attorney–client privilege. Violations of Russian law concerning attorney–client privilege and involving advocates is now rare.

In view of the above, and taking into account the unpredictable law enforcement environment in Russia, it is not surprising that companies hire advocates to conduct internal investigations.

Self-reporting under Russian law

In 2018, Russian law was updated to include provisions as to the voluntary disclosure of corruption offences by companies[21] (a similar provision of self-reporting agreements violating antitrust law had been part of Russian law since 2017).[22]

18 See, for example, Resolution of the Constitutional Court No. 33-P dated 17 December 2015.

19 ECHR judgment dated 4 February 2020.

20 In the case in question, the investigating authorities had obtained judicial authorisation for the searches in respect of the advocates, in accordance with the procedure prescribed by law. E.g, para 121, 122, 137 of the ECHR judgment re: Kruglov and others v. Russia dated 4 February 2020.

21 Article 19.28 of the Russian Administrative Code, note 5.

22 Article 14.32 of the Russian Administrative Code, note 5.

In particular, companies are released from liability for a corporate corruption offence if they contributed to the uncovering of the offence, assisted in the administrative investigation or the uncovering and investigation of the crime, or if they faced extortion. At the same time, Russian law contains no liability for the non-reporting of corruption offences.

The enforcement practice around these new legal provisions remains inconsistent. We are aware of a number of cases in the past year where the courts applied this provision to release companies from liability, but we have also seen cases where courts declined to apply this provision in seemingly similar circumstances. The enforcement authorities have not issued any guidance for evaluation of a company's efforts towards self-reporting and, in their public presentations, have mostly concentrated on the proper timing of self-reporting.

As to the timing, a decision to release from liability on the ground of self-reporting can be taken either by the enforcement authorities at an early stage of proceedings under the Code of Administrative Offences, or by the courts in the subsequent public proceedings. Thus self-reporting could very easily lead to no benefit at all if the prosecutor declines to release the company from liability and proceeds to bring the case to court

Clearly companies should carefully consider the risks related to self-reporting on a case-by-case basis. Among the other factors to be taken into account are the following:

- commencement of a criminal investigation into corruption involving employees of the company or business partners;
- known facts of self-reporting of a suspected individual in his or her personal capacity;
- disruption to business, caused by various investigative measures;
- self-reporting triggers under applicable anti-corruption laws in other jurisdictions; and
- the potential amount of the fine that could imposed for the offence (fines could reach 100 times the amount of a bribe or proposed bribe).

Conclusion

To some, the very notion of comprehensive anti-corruption legislation and compliance practices in Russia may come as a complete surprise, but only if you happened to have missed out on the fact that Russia's days as 'the Wild East' are many years behind it. This is not to say that Russia will likely be making a rapid climb up the Transparency International Corruption Perceptions Index any time soon. What it does mean, though, is that, in driving home the message of ethical business practices and the importance of eradicating bribery and other forms of corruption, a multinational corporation no longer has to reference the FCPA or the UK Bribery Act but can reference instead the (almost identical) obligations of the business under Russian law and the substantially similar local guidance as to meeting those obligations.

Paul Melling
Baker McKenzie

Paul Melling is an English solicitor who has spent his entire professional career working in the countries of the former USSR, having opened Baker McKenzie's Moscow office in January 1989. He has been resident and practising law in Moscow for over 30 years. In addition to being the founding partner of Baker McKenzie Moscow, he also opened his firm's Almaty office in 1995. He is the founder and leader of Baker McKenzie's compliance and investigations group in Moscow. He is also honorary legal adviser to the British Ambassador to Russia and a member of the Advisory Council of the Russo–British Chamber of Commerce.

Paul is known particularly for his work with multinational corporations in the life sciences sector (both pharmaceuticals and medical devices). In *Chambers Europe 2020*, he is ranked as an 'Eminent Practitioner' in the life sciences section and, as far back as 2009, he received the Distinguished Service Award from the Association of International Pharmaceutical Manufacturers for his 'Outstanding Contribution to the Development of the Russian Pharmaceuticals Market'.

Roman Butenko
Baker McKenzie

Roman Butenko is an associate in Baker McKenzie's Moscow office and a criminal advocate admitted to the Moscow city bar. He specialises in the area of anti-bribery compliance and investigations, criminal law and dispute resolution. Roman spent around one year in the Washington, DC office of Baker McKenzie, where he advised and assisted clients on various anti-bribery compliance matters. He also gained the unique multicultural experience of advising and representing clients across Central Asian jurisdictions during his over two year-practice in Almaty, Kazakhstan. Roman has a PhD in law and is a visiting lecturer at the Russian Ministry of Economic Development, as well as at a number of leading Russian universities, where he lectures on anti-corruption compliance matters. In 2019, Roman co-authored a major research paper for Baker McKenzie on the topic of corporate anti-corruption enforcement in Russia.

Ekaterina Kobrin
Baker McKenzie

Ekaterina Kobrin is a senior associate with Baker McKenzie in Moscow, working exclusively in the firm's compliance and investigation practice in the region. Her focus is on compliance, investigations and risk management and she has extensive prior experience in litigation and arbitration. An experienced investigator, she has led investigations in the post-USSR region for global clients operating in pharmaceuticals, IT and telecoms, energy, mining and infrastructure industry, consumer goods and electronics manufacturers, fast food and retail chains, logistics and facility management providers. She has handled matters involving bribery, fraud and conflicts of interest allegations, ethics violations and antitrust compliance cases. She also advises on privacy and data protection and is an expert on the legal aspects and practical challenges of forensic data collection, including those cases with complex privacy concerns.

Oleg Tkachenko
Baker McKenzie

Oleg Tkachenko is an associate with the Moscow office of Baker McKenzie and a Russian advocate. He focuses on criminal law and procedure and also specialises in investigations and litigation. He obtained this status and was admitted to the Moscow Region Advocates Chamber in 2004. Oleg is a former tax police officer. He worked at the Central Office of the Russian Tax Police from 2001 until 2004. His experience includes defence in a wide range of criminal cases, representation of victims, as well as assisting with searches and seizures, interrogations and internal investigations. Oleg is recommended for criminal proceedings and white-collar crime related issues by *The Legal 500 EMEA 2020*.

For more than 70 years, Baker McKenzie has been effectively providing global advice for large domestic and multinational clients and for over 30 of those years providing such advice in Russia. The size and global reach of our firm, with its 78 offices in 46 countries, guarantees that know-how is shared among jurisdictions and allows resources from our international network to supplement local office needs. Our lawyers advise clients on criminal and criminal procedure law issues, represent clients and their management before law enforcement authorities and regulators and lead internal investigations in response to allegations of the violations potentially leading to criminal and administrative liability (white collar crimes). Baker McKenzie was ranked as a leading law firm in Russia for its white collar crime practice in *The Legal 500 EMEA 2020*.

White Gardens
10th Floor
9 Lesnaya Street
Moscow 125196
Russia
Tel: +7 495 7872700
www.bakermckenzie.com

Paul Melling
paul.melling@bakermckenzie.com

Roman Butenko
roman.butenko@bakermckenzie.com

Ekaterina Kobrin
ekaterina.kobrin@bakermckenzie.com

Oleg Tkachenko
oleg.tkachenko@bakermckenzie.com

As well as daily news, *GIR* curates a range of comprehensive regional reviews. This volume, the *Europe, Middle East and Africa Investigations Review 2020*, contains insight and thought leadership from 32 pre-eminent practitioners from these regions. Inside you will find chapters on France, Germany, Italy, Nigeria, Romania, Russia, Switzerland and the UK (from multiple angles), the new fronts in fight against money laundering, how to 'remediate' in Africa – and lots more.

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

ISBN 978-1-83862-269-5