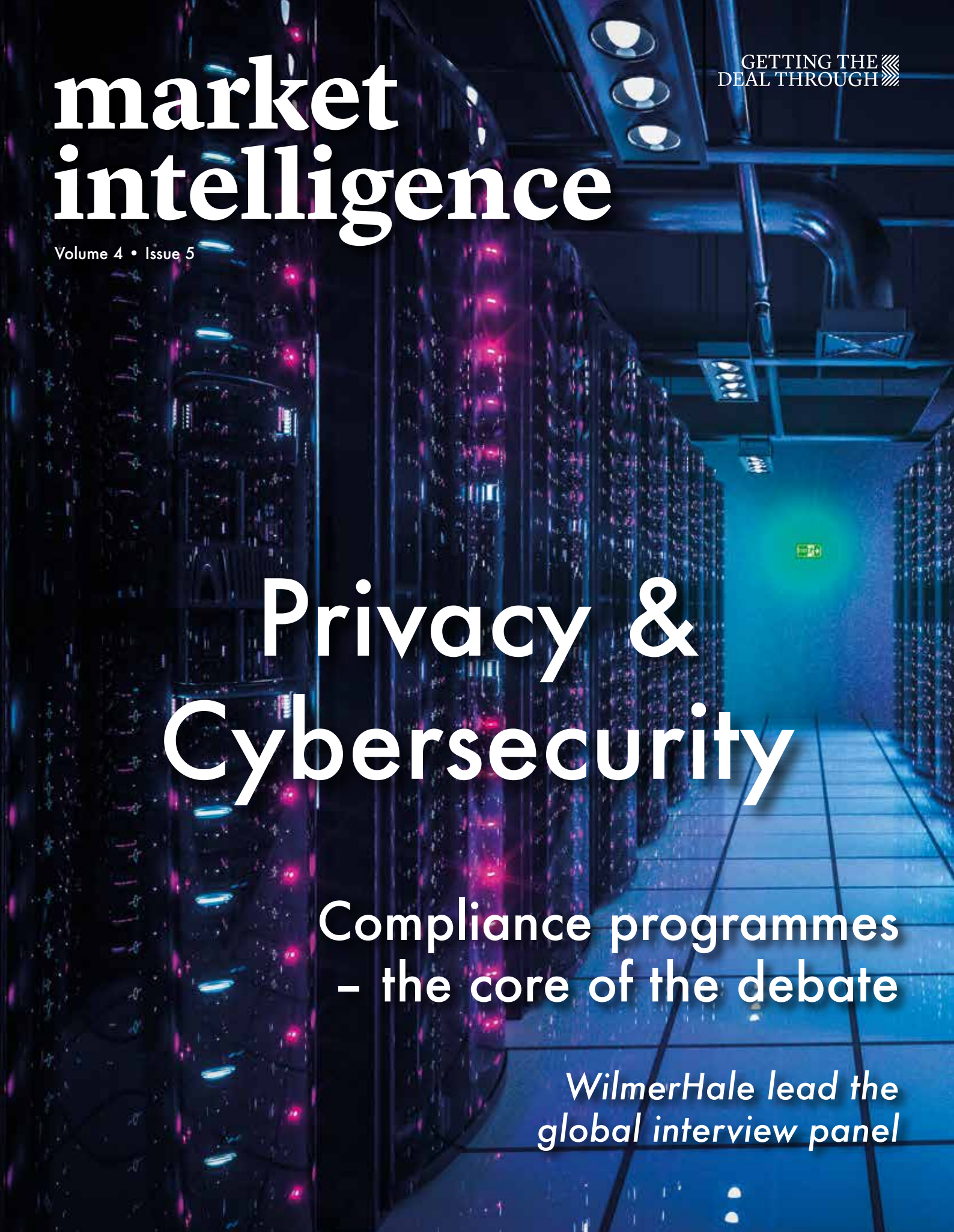

GETTING THE DEAL THROUGH

market intelligence

Volume 4 • Issue 5

Privacy & Cybersecurity

Compliance programmes – the core of the debate

WilmerHale lead the global interview panel

North America • Asia-Pacific • Europe • Latin America
Regulatory developments • M&A risks • Best practice • Cloud computing

Publisher: Gideon Roberton
Senior business development manager: Adam Sargent
adam.sargent@gettingthedealthrough.com
Business development manager: Dan Brennan
dan.brennan@gettingthedealthrough.com
Readership development manager: Rosie Oliver
rose.oliver@gettingthedealthrough.com
Product marketing manager: Kieran Hansen
subscriptions@gettingthedealthrough.com

Head of production: Adam Myers
Editorial coordinator: Gracie Ford
Subeditor: Jonathan Allen
Designer/production editor: Tessa Brummitt

Cover: iStock.com/4X-image

Law Business Research

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3780 4104
Fax: +44 20 7229 6910

ISSN: 2515-3749

GETTING THE DEAL THROUGH
Strategic Research Sponsor of the ABA Section of International Law

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

market intelligence

Welcome to GTDT: *Market Intelligence*.

This issue focuses on privacy and cybersecurity.

Getting the Deal Through invites leading practitioners to reflect on evolving legal and regulatory landscapes. Through engaging and analytical interviews, featuring a uniform set of questions to aid in jurisdictional comparison, *Market Intelligence* offers readers a highly accessible take on the crucial issues of the day and an opportunity to discover more about the people behind the most interesting cases and deals.

Market Intelligence is available in print and online at www.gettingthedealthrough.com/intelligence.

Getting the Deal Through
London
August 2017

In this issue

PRIVACY & CYBERSECURITY IN
RUSSIA

Vyacheslav Khayryuzov heads the IT, outsourcing and data privacy practice in the Noerr Moscow office, and advises clients in the technology, retail and media sectors. He is experienced in international IT and software law, data privacy and regulatory issues, as well as commercial, IP and media law issues in Russia. He represents national and international clients, from start-ups to large corporations.

Vyacheslav was recommended for TMT in Russia in *The Legal 500 EMEA* in 2016 and 2017, which stated: 'Noerr's Vyacheslav Khayryuzov has an excellent knowledge of privacy and data protection law and provides advice that considers business needs.' He has also been recommended in *Chambers Europe*, which states: 'Sources note he is clear in his assessment of possible risks and very practical'. Since 2012, he has been named among the world's leading lawyers in TMT by *Who's Who Legal*. The Who's Who Legal *Russia Special Report* 2014 described Vyacheslav, among other things, as "simply fantastic" and having a "brilliant way with clients". He has also been listed among the best lawyers for IT Law in Russia in *Best Lawyers* 2014–2018.

GTDT: What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

Vyacheslav Khayryuzov: The topic of cybersecurity is becoming a focus of discussions in Russia. The first thing that comes to mind is the alleged Russian hacking of the US presidential elections. The US media reported that the Obama administration was contemplating an unprecedented cyber covert action against Russia in retaliation for alleged Russian interference in the election. At least according to the media, the CIA has been asked to deliver options to the White House for a cyber operation designed to harass and 'embarrass' the Kremlin leadership.

Another infamous cybersecurity issue was the ransomware attacks WannaCry and Petrwrap/Petya. Major Russian and Western companies working in Russia were paralysed by the attacks for several days.

All these security issues have supported calls for Russia's internet infrastructure to be protected. As a consequence, the Russian parliament is currently considering a new draft bill on the security of critical information infrastructure of the Russian Federation. The draft bill sets out the basic principles for ensuring the security of critical information infrastructure, including the powers given to Russian state bodies to do so, as well as the rights, obligations and responsibilities of persons holding rights of ownership or other legal rights to the facilities for critical information infrastructure, communications providers and information systems providing interaction with these facilities.

The elements of the critical information infrastructure are understood to be information systems and telecommunication networks of state authorities, as well as automatic systems for the management of technological processes that are used in the state defence, healthcare, transport, communication, finance, energy, fuel, nuclear, aerospace, mining, metalworking and chemical industries. All these industries are considered critical for the economy and should be protected against any cyberthreats.

Obviously, living in the information society results in the overwhelming majority of decision-making and business processes in key economic sectors and governmental areas being implemented or planned using information technology. A significant portion of such information concerns spheres of particular importance to the state, including politics, national defence, finance, science and technology and the private lives of citizens.

In parallel, information technology is being widely introduced into automated production and process management systems for fuel and energy, finance, transportation and other sectors of critical infrastructure in Russia.


Vyacheslav Khayryuzov

As a result of the globalisation of modern information and communication networks and systems, Russia has had to switch to foreign equipment and imported software when developing such networks and systems. The overall load borne by such systems is increasing along with various information exchanges and tasks, and such systems use automated algorithms for production and process management accompanied by highly sophisticated information and communication channels. Such equipment and software is not always completely safe and has certain vulnerabilities. Therefore, the potential abuse of such systems for illicit purposes poses new security risks to the government and to businesses. As a result, Russian authorities have introduced rules requiring foreign software producers to allow the agencies certified by Russian state authorities to review the source code of the software (in most cases security products such as firewalls, anti-virus applications and software containing encryption) before permitting the products to be imported and sold in the country. This is done to ensure that there are no 'backdoors' in the software that could be used by foreign intelligence services.

Given that critical infrastructure links major national industries, any harm done to such infrastructure will inevitably harm these industries and the economy as a whole. Malware designed to modify binary code can disable any equipment that operates using binary code. At the same time,

attacks carried out for criminal, terrorist and intelligence purposes by individuals, communities, foreign special services and organisations are an equally serious threat. According to the media, the damage caused by malicious software worldwide totalled between US$300 billion and US$1 trillion (this is up to 1.4 per cent of global annual GDP), and there is still a steady upward trend in these figures.

GTDT: When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

VK: This is an interesting topic, since Russian data breach notification rules differ from European rules, and sometimes it is difficult to see the logic of these rules. It is generally accepted in Russia that Russian data protection law was highly inspired by European law. This is obvious when studying the Russian law on personal data. However, it appears that the concept of data breach notification was simply misunderstood by Russian lawmakers. As a result, there is no data breach notification requirement under Russian law, at least as it is understood in some other jurisdictions. As part of its data protection law, there is a requirement to notify individuals and the data protection authority on the resolved breach if a breach was found by an individual or the data protection authority and they requested that it be resolved. Data operators must notify individuals whose data was breached or the data protection authority if either of those parties requested the breach be resolved. This means that the authority or the individuals need to know that there was a breach. If they do not know about the breach, practically speaking, this means that companies can relax and do nothing – at least in this respect, as other Russian data protection rules are fairly burdensome – unless they are requested by the authority or by an individual to notify them of the resolved breach.

"It is practically impossible to stay completely protected from any cybersecurity threat."

GTDT: What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

VK: The biggest issues are not fines or any other regulatory consequences, as some people may think. Dealing with the data protection authority in the event of a data security incident may be cumbersome and result in fines (which are fairly small – up to approximately US$1,000), but it will not be more than that. The biggest threat is potential damage to reputation. In May, the WannaCry attack infected thousands of computers worldwide, and some law firms started to share their expertise in cybersecurity compliance, offering solutions for affected companies, including crisis management teams and even hotlines. After the mentioned attack of Petya on a major US law firm it may well be the case that clients in future would think twice before asking this law firm for cybersecurity advice. The damage to the firm's reputation is considerable and to be quantified. On the other hand, it is obvious that in the modern world it is practically impossible to stay completely protected from any cybersecurity threat. Even companies that consider cybersecurity to be of utmost importance are still vulnerable to cybersecurity attacks owing to the simple fact that they use information technology in their daily business.

GTDT: What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

VK: As a rule, Russian companies need to ensure that their systems in Russia are compliant with the technical requirements of the Federal Security Service of Russia and the Federal Service for Technical and Export Control of Russia (FSTEC). When setting up an IT system and related IT compliance procedures it is advisable to seek the assistance of a company that specialises in IT security and that has an FSTEC licence to carry out work related to data security (ie, protection of confidential information). An IT security company can also assist with preparing internal documentation, such as documents on technical issues of personal data protection, description of the IT security infrastructure and the measures to be taken by the company to prevent data breaches (eg, threat models, technical assignments). They can also advise on which hardware and software needs to be installed in order to ensure data security. At this stage of development of IT technologies it is highly advisable not to rely on one's own IT resources, but to use an outsourced provider of IT security services and let the professionals build the data security 'walls' of the company.

GTDT: Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

VK: The main concern is the infamous data localisation. As a result of the recent data localisation law, the collection of personal data from Russians and further direct storage in a cloud located abroad is no longer permitted.

The law created a new procedure blocking access to websites violating Russian laws on personal data and imposed a requirement to store the personal data of Russian citizens on servers located in Russia (which has given a huge boost to the development of the Russian data centre industry).

The personal data of Russian citizens must be stored and processed using databases located in Russia. The requirement can be complied with by placing the website database with the personal data in a Russia-based data centre or server. This database must be primary and the foreign cloud has to be the 'secondary' database, (ie, only a partial or full (mirroring) copy of the primary Russian database). This essentially means that the initial hosting must be located in Russia. Localisation of data is only one of a number of steps that need to be taken to ensure compliance. For instance, the consent of individuals must be obtained unless certain exemptions clearly apply. In most cases, consent must be given in writing (which means handwritten). In the event of cross-border transfers, the transferring entity in Russia needs to check whether the country of the data recipient is deemed to provide adequate protection to personal data, and if it is not, the consent of the data subject must also contain a specific authorisation to transfer personal data to such a country. For instance, transfers to the US or Canada require the explicit handwritten consent of the data subject for such a transfer. Apart from that, the transferring entity should consider entering into data transfer agreements, updating their cybersecurity procedures, etc.

GTDT: How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

VK: The government is very keen to combat cybercrime and is even imposing various rules in the laws aimed at increasing the cybersecurity for businesses. For instance, all companies dealing with personal data must apply certain technical and organisational measures aimed at protecting data and use software certified by Russian authorities.

Any computer fraud, unauthorised data access or creation of malicious software may result in criminal liability. However, the actual number of hackers being convicted is fairly low. The reason for this is unclear and certainly gives rise to speculation.

"The actual number of hackers being convicted is fairly low. The reason for this is unclear and certainly gives rise to speculation."

Russia refused to ratify the Council of Europe's Convention on Cybercrime and, based on the discussions within the Russian government, it appears that this will remain the case. The government's officials claimed that they do not agree with the convention's provisions for the sanctioned access of one member state to computer data stored in the territory of another member state without the prior consent of the latter. The officials justify this on grounds of national security.

State officials have said that Russia's approach to combating cybercrime consists of 'the prompt and adequate cooperation of law enforcement authorities of different countries, as well as of the non-admission of investigations on a foreign territory without the notification of the law enforcement authorities of the state concerned'. Moreover, the authorities believe that Russia is considering promoting an approach that provides for the development of a global convention on combating crimes in the information sphere instead of the Budapest Convention, which only applies regionally and will not be as effective as possible. Following a proposal put forward by Russia, in May 2010 the UN Commission on Crime Prevention and Criminal Justice established an intergovernmental expert group to draft proposals to improve the international legal framework in this sphere.

GTDT: When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

VK: Apart from standard confidentiality and privacy precautions such as encrypted data rooms and non-disclosure agreements, companies entering into M&A deals in Russia should consider

THE INSIDE TRACK

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

Because every cyberattack is unique, and there are many different, rapidly emerging cyberthreats, there is no standard approach for selecting the best legal adviser. The following attributes could be useful:

- Russian market knowledge and close cooperation with IT security firms. Furthermore, lawyers can only be valuable in cybersecurity practice if they cooperate with a team of IT security specialists, preferably licensed by the FSTEC.
- Fast response by lawyers and IT specialists 24/7 and 365 days a year can be crucial in a cyberattack. Look for a reliable partner who can help build cybersecurity (including legal organisational and technical IT measures) from scratch or help fine-tune procedures to the Russian market.
- Look at the law firm's portfolio of completed cybersecurity risk management projects.
- Perform a threat modelling exercise and expose the whole team (IT, PR, finance, legal) to a mock cyberattack to see how it would be dealt with in real life.

What issues in your jurisdiction make advising on privacy and cybersecurity complex or interesting?

Russian laws (not just on privacy and cybersecurity) are changing rapidly, which is a big problem for businesses on the one hand, since they need to adjust quickly to the unstable legal framework, and on the other hand makes advising on this issue very interesting. Since 2014, Russia has adopted many new privacy and cybersecurity laws. Most of these laws were rough and not suitable for use and even law enforcement agencies struggled to interpret the rules and clarify to businesses what future enforcement would be like. Advising in such circumstances is like stumbling around in the dark, trying to find the right answers. It requires cooperation with the authorities and tracking all the latest enforcement cases. It makes advising on privacy and cybersecurity fairly complex, but extremely interesting.

How is the privacy landscape changing in your jurisdiction?

Since 2014 Russia has adopted many laws on privacy and cybersecurity. The data localisation law now requires storage of Russian citizens' personal data on servers located in Russia. In June 2016 the parliament adopted the Federal Law on Amendment of the Federal Law on Counterterrorism and Related Laws of the Russian Federation Establishing Additional Counterterrorism and Public Security Measures (the Yarovaya law). These amendments introduced changes to Russian legislation related to telecommunications and the internet. For instance, the law requires Russian communications service providers to store all information on their customers' and internet users' communications in Russia for specified periods.

The substitution of foreign software imports is another trend. The government created a register of Russian software and requires state agencies to purchase Russian software instead of foreign software, unless the authorities can prove the software has no equivalent in Russia.

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

Cybersecurity threats in Russia are generally similar to those elsewhere in the world. Distributed denial-of-service attacks and ransomware attacks are very common on the market and companies need to be prepared for them. However, the authorities are creating many obstacles in the regulation of privacy and cybersecurity and this should also be considered a point of risk for businesses. Companies coming to do business in Russia should also realise that data access requests from various state agencies (not only state security agencies) are not uncommon and the extent of the information that can be given to the authorities should always be considered carefully; this is where the advice of a competent lawyer is particularly useful.

Vyacheslav Khayryuzov
Noerr
Moscow
www.noerr.com

personal data transfer issues before starting the due diligence process. As previously mentioned, owing to the recent data localisation law, the collection of personal data of Russians and further direct storage in a cloud located abroad is no longer permitted. Therefore, a potential foreign purchaser should double check whether personal data (eg, of the employees of the target company) is stored in a Russian primary database and whether the relevant consent given by such employees to the seller allows for the transfer of their data to the purchaser. Violation of these rules may result in negative consequences for the purchaser since, in certain circumstances, Russian data protection authorities can even block access to the purchaser's website as a part of enforcement actions.

Also available online

www.gettingthedealthrough.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

Official Partner of the Latin American Corporate Counsel Association

ABA Section of International Law
Your Gateway to International Practice

Strategic Research Sponsor of the ABA Section of International Law