E-BOOK:

LEGALLY OBTAINABLE DATA IN BRIC COUNTRIES

STEELE

CONTENTS

Introduction to Anti-Bribery and Anti-Corruption Compliance

Complying with Anti-Bribery and Anti-Corruption (ABAC) regulations involves many critical steps, none more important than the performance of third-party due diligence. Given the number of cases involving the use of third parties to facilitate bribes, to avoid regulatory scrutiny companies must dedicate the time, effort, and resources to vet each entity they engage.

Inevitably, investigating third parties requires gathering and analyzing personal data. Unfortunately, while conducting initial and ongoing due diligence of their third parties, a company may end up violating one or more data privacy laws. To complicate matters further, data privacy laws vary drastically by country.

Changes in global data privacy regulations present challenges for corporate compliance departments. Complying with constantly changing regulations requires an understanding of the myriad of laws in numerous countries and the steps needed to comply with those laws.

Companies seeking to comply with ABAC regulations must be able to conduct reasonable, risk-based due diligence of their third parties. Such due diligence requires vetting third parties and their principals. Implementing a robust third-party due diligence program depends on access to data. Typically, in order for a corporation to vet its third parties without violating the country's data privacy laws, the corporation must possess a detailed understanding of the obligations that come with access to personal data.

In order to help companies navigate this complex environment, STEELE CIS prepared a series of articles relating to data privacy laws in Brazil, Russia, India, and China (BRIC). Each article provides the following:

- An overview of each country's data privacy laws and regulations.
- A detailed discussion of what constitutes legally obtainable data in each market.
- The types of consent required from the data subject.
- A discussion of the challenges companies face when conducting third-party due diligence in the BRIC countries.
- The role of private investigators in the third-party due diligence process.

< back to top

BRAZIL

Like many countries, Brazil has chosen to address data privacy through general and sector-specific laws, rather than by approving a single all-encompassing law. Therefore, multinationals that want to ensure they are in compliance with Brazil's data privacy laws must possess the ability to navigate the country's patchwork of contradictory requirements.

As a standard compliance practice, companies operating in Brazil should rely on suitably qualified due diligence firms with local in-depth knowledge of how to investigate third parties to ensure they do not run afoul of Brazil's data privacy laws.

Brazil's Legal Landscape

Personal information in Brazil is directly or indirectly governed by the:

- Federal Constitution.
- Civil Code.
- Consumer Protection and Defence Code.
- Federal Act 9296/96.
- Federal Act 12.414/11.
- Internet Act.
- Access to Information Act.

Of this legal landscape, the three most relevant laws regarding third-party due diligence are the Federal Constitution, the Civil Code, and the Consumer Protection and Defence Code.

The Federal Constitution

Stipulates that the right to privacy and secrecy of communications are among a citizen's fundamental rights. However, it does not codify how a citizen may ensure their rights beyond their ability to claim such rights. The Civil Code broadens the narrow definition included in the Constitution to include remedies that an individual may pursue for data privacy violations. Also, Federal Act 9296/96 regulates the interception of computer and telephone traffic, in accordance with the provisions of Federal Constitution. According to this act, in the absence of an injunction, intercepting such data is a felony.

The Consumer Protection and Defence Code

Addresses consumer privacy and includes a section that grants consumers access to data about them. It stipulates that the consumer must have the option to make changes to the data or request its deletion. Still regarding consumer protection, Federal Act 12.414/11 regulates databases used to conduct credit analysis. It encompasses concepts such as sensitive data, but is limited to provisions related to consumer databases.

The Internet Act

Governs the collection, use, and storage of personal data involving the Internet. Recently, Decree 8771/16 regulated the Internet Act, indicating, among other aspects, procedures related to data protection.

The Access to Information Act

Relates to data about individuals that is stored by government agencies. The law provides individuals with the ability to request access to the data stored on government databases and the right to request removal of data incorrectly stored under their name. This access applies specifically to data that either belongs to or can be transferred to third parties. It does not apply to data that the government classifies as private for government use only.

While Brazil currently lacks a law that presents a unified approach to data privacy, and the applicable law(s) vary based upon the circumstances, companies should assume that in order to conduct third-party due diligence and process Personally Identifiable Information (PII), they must secure the subject's consent. Failing to follow this simple step may expose both the data controller and the processor to unspecified penalties.

Although not specifically stated in Brazil's legal codes, most data privacy laws define a data controller as an individual, company, or organization that determines the purpose and manner in which data is processed. Similarly, a data processor is an individual, company, or organization that processes data on behalf of a data controller.

Personally Identifiable Information

Similar to data privacy laws in the United States, Brazilian law does not present a fully comprehensive definition of PII—at least not yet, considering the lack of a general law regarding protection of personal data. Consequently, what constitutes PII will vary by applicable sectorial laws and court's interpretation.

Regarding sectorial laws on the matter, it is important to notice the above-mentioned Decree 8771/16, which establishes the definition of registration data (i.e. parent's name; address and personal qualification) and personal data (i.e. data related to the identified or identifiable individual, including identification numbers, locational data or electronic identifiers, when these are related to one person). However, these definitions are only applicable when data processing involves the Internet.

Furthermore, the country's Civil Code refers to the protection of an individual's private life and intimacy. Therefore, the Civil Code is by definition broad and all-inclusive.

Absent a general, clear and compelling definition regarding what data constitutes PII, multinationals should employ a broad approach to classifying data gathered during the course of third-party due diligence, respecting the sectorial rules that may apply to the process.

Efforts are underway in Brazil to create a comprehensive personal data protection law. Therefore, the Personal Data Protection Bill (Bill 5276/16) is currently pending before Brazilian National Congress and will probably modify the above presented scenario regarding processing of personal data.

< back to top

Conducting Due Diligence in Brazil

Conducting third-party due diligence involves gathering data regarding the entity and its principals. In Brazil, as part of their due diligence efforts, companies may analyze data regarding a third party's shareholders, key management, business partnerships or affiliations, as long as that information is not private or secret and is publicly available.

As a general guide, companies may use the following types of data as long as it is publicly available:

- Civil litigation and criminal complaints.
- Legal judgments and other filings.
- Corporate registration data.
- The entity's legal structure.
- Credit, banking, and financial information.
- Official records of regulatory citations or fines.
- A principal's professional reputation.
- Information reported on local blogs, social media, and online forums.

Those involved in requesting and conducting third-party due diligence must understand their rights and obligations regarding the handling of PII. While Brazil's patchwork of data privacy laws does not include a set of remedies that apply to all companies and industry sectors, in the event that a multinational violates data privacy law the courts and the Ministry of Justice may assess penalties based on the specific fact relating to the violation.

< back to top

The Role of Private Investigators

Private investigators may gather publicly available information. They do not have the authority to request any other type of data unless engaged to obtain information and documents as part of the due process associated with a lawsuit.

Companies and their private investigators do not have access to Brazil's national criminal records database. However, as part of the hiring process for certain positions such as security guards, for example, companies may seek cooperation from the candidate to conduct a search of the country's criminal records database. This involves the candidate obtaining a criminal records report from the government and, subsequently, providing that report to the hiring entity. Third parties cannot initiate such a request.

While not expressly prohibited by law, companies should refrain from using health-related information or any other data that could lead to prejudice. This is consistent with the general EU prohibition on processing "sensitive data."

Licensing Requirements

Brazil does not regulate the private investigator profession. Consequently, private investigators in Brazil do not need a license to conduct an investigation, nor must they adhere to a commonly accepted body of professional standards.

Without a licensing and disciplinary body and the lack of professional standards, engaging a private investigator presents multinationals with challenges in maintaining compliance with relevant laws and ensuring the quality of the investigations conducted.

Consent and Recordkeeping

Conducting third-party due diligence involving PII requires the data subject's consent. In fact, in order to minimize legal risk, companies must obtain consent whenever they process personal data.

While the law does not specify how a data controller or a data processor secures such consent, any agreements with a third party and its principals should clearly detail the data involved in the due diligence process. The controller or processor also should secure explicit consent to proceed. Such an agreement should specify the intended use of the data, including how the data controller and the processor plan to protect and disseminate the information.

Also, Brazil's Internet Law broadly describes the consent required to release personal data to third parties as express consent provided freely by informed parties. To that end, to comply with this law, pre-formulated standard agreements must separate and highlight the consent clause.

A multinational can send PII outside of Brazil if they obtained the party's express consent to send their data overseas.

Unless prescribed otherwise in law, if a data subject changes their mind and withdraws consent to process their personal information, a company must stop processing the data immediately. Given the lack of a comprehensive data privacy law that defines the roles of the data controller and the processor, investigators should consider providing consent disclosure in both English and Portuguese. This can help minimize confusion and prove to a court that the data subject received notice in their native language and, therefore, conceivably understood and granted their consent with full knowledge.

< back to top

Challenges for Investigations: Brazil's Size and Pervasive Corruption

With a population of just over 200 million spread across 3.29 million square miles, conducting investigations in Brazil presents many logistical challenges. Consequently, multinationals may struggle to source a firm with the ability to conduct due diligence throughout the country.

The sheer size of the country is not the only issue facing multinationals. In its 2015 report, Transparency International, a non-governmental entity that tracks and reports corporate and political corruption around the globe, Brazil ranked 76th on a list of 168 countries. In the same report, the United Kingdom ranked 10th; the United States, 16th; and China, 83rd. Therefore, multinationals must consider the presence of corruption and engage private investigators who agree to comply with relevant laws, including, for example, the U.S. Foreign Corrupt Practices Act (FCPA).

RUSSIA

The Russian Federation Federal Law of 27 July 2006 N 152-FZ governs the use of personal data (the "Personal Data Law"). It may affect a multinational's ability to collect and process personal data and remain in compliance with Anti-Bribery and Anti-Corruption (ABAC) regulations.

When conducting third-party due diligence, companies should use only that information which is allowed under data processing regulations. As a general principle, legally obtainable information is data that is publicly available without the consent of the subject of that information. If the subject cannot gather the same information about himself or herself, it is potentially illegal to process that data.

Russia's Legal Landscape

Data privacy includes the tools and tactics used to gather, store, and disseminate sensitive data, such as personally identifiable information (PII), in a manner consistent with data protection laws and regulations. In order to avoid violating Russian Personal Data Law, before a company conducts third-party due diligence, its representatives must understand their rights and obligations with respect to the gathering, usage, and storage of data. The law includes the principles and conditions governing the processing of personal data, the type of individual consent required, and the obligations of the entities that gather personal data.

The Russian Personal Data Law follows many of the principles found in modern data protection or data privacy laws and the Safe Harbor Principles, including the definition of personal data, restrictions on the processing of sensitive data, and requirements for notice and consent. The law defines personal data as "any information referring directly or indirectly to a particular or identified individual (hereinafter referred to as 'personal data subject')."

Under the Russian Personal Data Law, the party conducting or directing the processing of personal data is the "operator." The law states that an operator "shall have the right to assign the processing of personal data to another person with the consent of a personal data subject."

Further, "A person carrying out the processing of personal data on the instruction of an operator shall not be obliged to obtain the consent of the data subject to the processing of his personal data." The law allows for the processing of personal data where "required for performance of an agreement to which a personal data subject is a party or under which the data subject is a beneficiary or surety, or for conclusion of an agreement on the initiative of a personal data subject or an agreement under which a personal data subject shall be a beneficiary or surety."

The law also allows for the processing of personal data where "processing of personal data is required for realization of the rights and legitimate interests of an operator or third parties for the attainment of socially significant objectives, provided that this does not cause the rights and freedoms of the personal data subject to be violated." In short, the law may complicate a multinational's attempts to conduct meaningful due diligence on individuals.

< back to top

Securing a Data Subject's Consent under Russian Law

Under the Russian Personal Data Law, "a personal data subject shall decide whether or not to provide his personal data and shall give consent to the processing thereof freely, of his own will and in his own interest."

> *"Consent to the processing of personal data shall be specific, informed and conscious."*

The Russian Personal Data Law assigns the burden of proof regarding consent to the operator—record keeping of consent receipts, therefore, is vital to the due diligence process. Fortunately, the law allows for some processes that may expedite the consent receipt process.

- Consent in the form of an electronic document signed with an electronic signature is equivalent to a written consent on paper containing the handwritten signature of the personal data subject.
- The personal data subject or his representative may give consent to the processing of personal data in any form that provides evidence of its receipt.
- When dealing with an intermediary who represents the personal data subject, companies should confirm the intermediary's authority to provide consent on the personal data subject's behalf.

Importantly, the Russian Personal Data Law requires written consent to contain the following:

1. Name, address, and principal identification document (and issue date and issuing authority) of the personal data subject.
2. Name and address of the representative of the personal data subject, identification information about the representative, and details of the representative's authority.
3. Name and address of the operator.
4. The purpose of personal data processing.
5. A list of personal data for which consent has been given for processing.
6. Name and address of the person who is to carry out the processing on the instruction of the operator.
7. A list of actions involving personal data and the general description of methods of processing to be used by the operator.
8. The period for which the consent is given and the procedure for withdrawal of consent.
9. The signature of the personal data subject.

Challenges for Investigations: Key Considerations to Ensure Compliance with Russia's Data Privacy Law

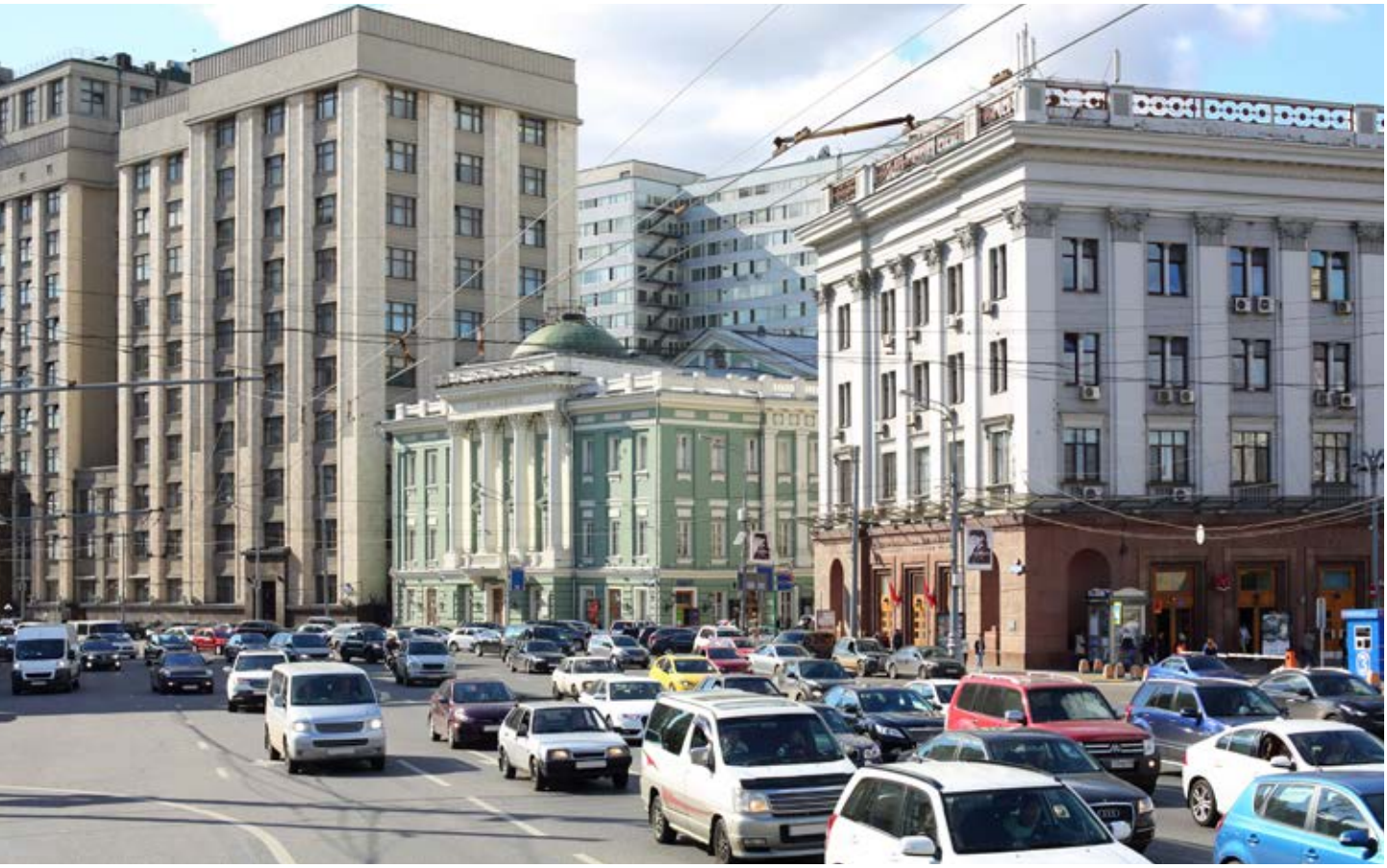
The consent provisions of the Russian Personal Data Law are onerous, administratively burdensome, and call for automation if a company has a large population of Russian personal data subjects on whom to conduct due diligence.

For companies that rely on a third-party due diligence questionnaire ("DDQ") to obtain consent, that consent should list the types of personal data being processed.

Alternatively, a company could provide draft consent forms containing the nine elements of required information detailed above, including the identifying information of the firm conducting due diligence, as an addendum to the DDQ for completion by the personal data subjects. Scanned PDF versions of consents could be electronically transmitted back to the company or uploaded into its third-party management system.

Localization of Data on Russian Data Subjects

It is important to note that Russia's data localization law, Federal Law No. 242-FZ, was adopted as a set of amendments to Russia's On Personal Data Law in July 2014 and became effective on September 15, 2015. The law requires "operators" to collect, store, and process Russian citizen's personal data using databases located within Russia. Additionally, operators must also inform Russia's data protection authority, Roskomnadzor, or the location of the servers where Russians' personal data is stored. During meetings to explain their understanding of the localization requirement, representatives of Roscomnadzor commented that the localization requirement does not prohibit the transfer and storage of data abroad, but that the initial collecting of data from individuals and any updating of that data should be done through a database located in Russia. Accordingly, Roscomnadzor said that there should always be a database located in



Russia through which the initial input or any updates should pass in the first instance. After that, the data may be copied and transferred to foreign databases subject to compliance with cross-border transfer requirements – in particular, the cross-border transfer of such data should have the same purpose as initially declared when the information is collection, and written consent of the individual may be required in certain cases.

The Role of Investigators

First enacted in 1992, Federal Law No. 2487-I "On Private Detective and Security Activity in the Federation of Russia" (the "Private Detective and Security Law") governs the activities of private investigators. The law includes the requirements to become private investigators and the associated liability for illegal activities.

The Private Detective and Security Law allows citizens of the Russian Federation who have the appropriate license to conduct private investigations. Securing a license requires an individual to earn a degree or undergo special training as a private detective. Alternatively, an individual with three or more years of experience in state law enforcement or the security services may receive a license to conduct private investigations.

A license allows an individual to conduct private investigations within a specific territory of the Russian Federation. This includes the investigation of a company's third parties. In order to ensure compliance with the law, the private investigator must obtain written consent from their clients in accordance with the consent laws previously described.

Further, private investigators cannot collect information related to private life, political, or religious affiliations. Nor can they conduct audio, video, or photographic surveillance without a subject's consent.

In addition to the requirements and limitations detailed above, the law includes additional layers of restrictions relating to private investigations. Notwithstanding the compliance burden associated with the Russian Personal Data Law, the country's Private Detective and Security Law further complicates the regulatory landscape. This inherent complexity justifies involving experienced local experts to conduct the local aspects of ABAC due diligence.

Conducting Due Diligence in Russia

As it relates to the processing of personal data and third-party due diligence, the company, defined as the operator, is ultimately liable to the personal data subject for violations of Russia's Personal Data Law.

Therefore, when hiring a due diligence firm it is critical to ensure that they have the people, processes, and technology in place to process data on the operator's behalf and comply with Russia's Personal Data Law.

Ensuring that an organization maintains compliance with both the FCPA and Russia's Personal Data Law requires a working knowledge of both laws and the ability to engage the company's data privacy officer and counsel, as needed.

Local knowledge of the intricacies of Russia's Personal Data Law, the legality of data sources, and the level of enforcement play a critical role in ensuring that a company gathers data on a third-party's principals without infringing on that subject's rights.

INDIA

Despite several efforts to broaden and strengthen India's data privacy laws, companies conducting third-party due diligence in India face just two laws that apply throughout the country as well as sector-specific requirements within its banking sector. However, India's parliament is considering several regulatory laws, including one designed to place the country's data privacy laws on par with other developed economies.

India's Legal Landscape

The following laws control access and use of personal data in India:

- Information Technology Act, 2000 (Amended 2008)
- The Information Technology Rules, 2011

Similar to most countries, in addition to overarching laws that apply to all businesses, India's banking and finance regulators require entities under their authority to protect their customers' personal data.

Within the next year, India may enact a new law designed to prevent misuse of personal data by both the government and private organizations. The Right to Privacy Bill, 2014, which is still undergoing review and comments, aims to overcome political resistance that has stopped several privacy-related bills from becoming law.

Definitions Relating to Data Privacy

The Information Technology Act, as amended in 2008, requires the protection of Sensitive Personal Data or Information (SPDI). The amendment defines SPDI as "such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit."

However, in April 2011, the government released the Information Technology (reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. These rules provided the following definition and requirements of SPDI as it relates to the Act:

- Password.
- Financial information such as bank account, credit card or debit card, or other payment instrument details.
- Physical, physiological and mental health condition.
- Sexual orientation.
- Medical records and history.
- Biometric information.

- Any detail relating to the above clauses as provided to body corporate for providing service.
- Any information received under the above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.

While the IT Act includes dated terminology, the law still applies and, together with the IT Rules, governs how companies can gather, store, and disseminate personal data.

The 2008 amendment to the Information Technology Act strengthens the law and provides the following important definitions regarding the entities that fall within its scope and their responsibilities for ensuring security:

- Body Corporate: Any company, including a firm, sole proprietorship, or other association of individuals engaged in commercial or professional activities.
- Reasonable security practices and procedures: Security practices and procedures designed to protect information from unauthorized access, damage, use, modification, disclosure, or impairment.

Conducting Due Diligence in India

Notwithstanding India's size and the inherent difficulties that present when conducting due diligence, the country recognizes more than 20 official languages and in excess of 30 local dialects. Consequently, while performing due diligence in India, local investigators play a critical role. Not only do they possess the ability to communicate in the appropriate language, they understand the nuances of the culture in a particular region, which is a critical skill when attempting to discern whether a third party operates within the boundaries of the law.

To complicate matters further, India does not maintain national databases that investigators can depend upon for complete and accurate data. In turn, local investigators must conduct a series of searches of the relatively few local databases that exist online, as well as manual searches of records that government departments maintain. With each new search—either electronic or manual—the potential to mishandle data and violate the country's data privacy laws increases.

The Role of Private Investigators

India does not have a law that governs the conduct of private investigators throughout the country. India's central government created the Private Security Agencies (Regulation) Act, 2005, and encourages the states to adopt the law. However, the law remains largely unenforced. The Private Detective Agencies (Regulation) Bill, 2007, which is still under review, uses the Private Security Agencies (Regulation) Act, 2005, as its basis.

Licensing Requirements

While the country lacks a law that applies to private investigators operating in India, the 2007 Bill under review seeks to significantly increase the level of oversight and accountability of the private investigators and agencies. The Bill includes the following elements and highlights:

- Every private detective agency will require a license to operate.
- Licenses shall be granted by regulation boards established at the central and state level.

- Breaching of an individual's right to privacy carries a prison term, which may extend to six months, and a fine of up to fifty thousand rupees. The individual's agency also faces suspension or cancellation of its license.
- A private detective agency may employ a person as an agent if he is an Indian citizen of 21 years of age or above and satisfies certain training and physical fitness requirements.
- An agency must maintain a register with specified information, including the names and addresses of its managers, staff, and clients. It shall also record the salaries of its staff and the gist of the work it has undertaken for a client.

Consent and Record Keeping

A data subject must provide consent before a data controller can collect sensitive personal data or information. The subject may provide consent in writing—including via online channels. Consent must be expressed, not implied. Indian law does not specify the form of consent, and a data subject may withdraw their consent at any time. Upon notice of withdrawal (Indian law does not specify the format), both the data controller and processor must cease analyzing the data in question.

< back to top

CHINA

In October 2013, President Xi Jinping approved revisions to the Consumer Rights and Interests Protection Law of the People's Republic of China. This action represents the latest attempt to improve the country's approach to data privacy and protection. The new law became effective March 15, 2014.

This law includes the requirement that business operators keep personal information confidential and not disclose or illegally provide personal data to others. There also is a requirement to ensure information security and prevent inadvertent disclosure. In accordance with the Measures for Punishment of Infringements on Consumer Rights and Interests ("SAIC Measures") issued in March 2015, consumers' personal information includes "the information collected by business operators during the provision of goods or services that may be used for identifying a consumer either independently or in combination with other information, and shall include name, gender, occupation, date of birth, identity document number, residential address, contact details, income and asset conditions, health conditions and consumption habits of a consumer."

China started taking steps to protect consumer data in 2000 with the Decision of the National People's Congress Standing Committee on Safeguarding Internet Security. Because the country lacks a single, all-encompassing law that corporations can turn to for guidance and unified practice by various governmental authorities involved, China's mosaic of data privacy laws presents considerable compliance challenges for multinationals.

In order to comply with the Foreign Corrupt Practices Act (FCPA), for example, multinationals must conduct reasonable, risk-based due diligence of their third parties. In many cases, that requires due diligence on the principals of an entity, not just the entity itself. As an example of the issues that can result, organizations must ask themselves how they can conduct FCPA-related due diligence on Chinese principals without violating the country's data privacy laws in the process.

China's Legal Landscape

There are various laws and regulations in China that address data privacy or include provisions on protection of personal information. The following laws and regulations directly or indirectly address the protection of personal information in relation to the subject topic (various regulations in other areas such as telecom and internet are not particularly provided herein):

- Protection of Computer Information System Security
- The Law of The People's Republic of China on Resident Identity Cards
- The People's Court Disciplinary Measures
- Prosecutors Disciplinary Regulations
- Consumer Rights and Interests Protection Law

- Practicing Physicians Law
- Medical Institution Medical Records Management Regulation
- Commercial Banking Law
- Postal Law
- Regulations on the Real Name of Individual Deposit Account
- Law of Advocate
- The Archives Law

In fact, any law in China associated with personal information may include restrictions regarding the use and safekeeping of personal data. Since China does not have an all-encompassing data privacy law, complying with existing laws and the recently passed Consumer Rights and Interests Protection Law requires caution and in-depth knowledge of the country's legal environment.

Definitions Relating to Data Privacy Lacking

Data privacy includes the tools and tactics used to gather, store, and disseminate sensitive data, such as personal information in a manner consistent with data protection laws and regulations. In China, there is no universally accepted definition of data that constitutes personal information although it is normally considered that any information that can be used to identify an individual either alone or together with other information as personal information. In fact, many of the laws designed to prevent the theft and misuse of personal information in China lack clear definitions and parameters regarding what is acceptable, which, in turn, makes securing criminal convictions difficult to accomplish. Specific circumstances will also need to be considered to determine what information will be considered as personal information.

Conducting Due Diligence in China

FCPA-related due diligence typically focuses on a third party's principals. In order to conduct due diligence of third parties, such as accountants, acquisition targets, distributors, export agents, joint venture partners, lawyers, resellers, and vendors, companies need access to data.

As a general rule, corporations should only use legally obtainable information when conducting due diligence on entities and principals. The corporation also should obtain the consent of concerned individuals for collecting and using his personal information as required by law. If the subject cannot gather the same information on himself or herself, the data is potentially illegal.

Parties conducting due diligence must understand their rights and obligations with respect to the gathering, use, and storage of data. Although not clearly defined in Chinese law, a data collector is an individual, company, or organization that determines the purpose and manner in which data is processed normally deemed responsible for the collection and use of personal information.

The Role of Private Investigators

Thus far, Chinese law has not addressed the role of private investigators. The law does not prohibit private investigations, but it does not approve them either. Private investigators operating within existing

legal limits may go unnoticed. Alternatively, if the private investigator's activities violate the limit posed by laws, they may attract the attention of Chinese authorities.

Notwithstanding the inherent risk of conducting any form of investigation in China, to avoid attracting the attention of Chinese authorities it is critical to engage a company that understands data privacy regulations and the laws and practices set in place by regulatory bodies that oversee any journalist research and private investigation services. The Chinese government closely monitors those involved in due diligence in a manner similar to its monitoring of journalists.

In addition, since firms that conduct investigations in China do so under general business licenses, without specific qualification they are not required to satisfy professional standards, experience, and insurance coverage requirements.

To complicate matters further, at the beginning of 2013, the Administration of Industry and Commerce (AIC), which stores financial as well as ownership records for companies in China, restricted access to its records. Consequently, private investigators may resort to gathering data via other means that violate Chinese data privacy law if they wish to obtain information beyond public resources.

CONCLUSION

While the inherent compliance risk that each third party presents will dictate the scope of due diligence and, therefore, the types and volume of PII handled during the process, companies must avoid achieving compliance with ABAC law at the expense of data privacy law. In fact, conducting third-party due diligence should go hand in hand with satisfying data privacy compliance, and effective ABAC due diligence can be conducted without processing PII that is considered to be "sensitive data."

Preventing bribery without violating data privacy law requires local in-depth knowledge, as well as an understanding of the practical realities of conducting third-party due diligence in foreign markets. In order to avoid the unintentional misuse of personal data and maintain compliance with the country's data privacy laws and regulations, multinational companies must often comply with several regulatory laws, as well as numerous sector-specific requirements.

Now is the time for multinationals conducting third-party due diligence to ensure that their efforts to comply with ABAC regulations do not inadvertently violate one of the many laws relating to consumer data privacy.

AUTHORS

Renato Opice Blum, Partner, Opice Blum Law Firm

Renato is a partner with the law firm of Opice Blum Advogados Associados in São Paulo, Brazil, where he practices electronic, computer, and technology law. He is also an economist. Renato is the Digital Law Programme Coordinator of the MBA course on Information Technology Law at São Paulo Law School, and a Professor at Mackenzie University, the University of São Paulo, and Fundação Getulio Vargas (Getulio Vargas Foundation). He is the Vice President for the Brazilian Bar Electronic Law and High Technology Crimes Commission. He also is an international lecturer on topics in technology law, and he coauthored many articles and books, including the treatise , "Manual of Electronic Law and Internet" and "Electronic Law: Internet and Courts"; Co-author of the article "Recent Development on Cyberspace Law: A View from Brazil", and "Brazilian's Chapter" of Data Protection & Privacy Law (2nd Edition).

Durga Bose Gandham, Partner, Tatva Legal

Durga Bose Gandham is a partner with Tatva Legal, which is based in Hyderabad, India. His practice focuses on litigation and dispute resolution related to competition law, general corporate, arbitration, and banking matters. He has successfully represented Indian, U.S., Asia-Pacific, and European companies in issues related to antitrust law, commercial litigation, arbitration, intellectual property, employment and labor, FCPA, cyber law, real estate, debt recovery, and consumer laws and litigation related to criminal law.

Dennis Haist, General Counsel, STEELE CIS

Dennis Haist is general counsel and compliance advisor for STEELE CIS and its affiliated companies. Previously, Haist served as vice president and general counsel of Dillingham, an international engineering and construction company. He has developed corporate compliance programs and conducted internal investigations in the areas of anti-trust, FCPA and false claims.

Caroline Lee, Managing Director, STEELE CIS, Asia

Caroline Lee is managing director and regional compliance officer for STEELE CIS Asia Pacific Region (Hong Kong). For the last six years, Lee has managed the delivery of research operations and ABAC regulatory compliance in Greater China for large multinational companies in the medical-device and pharmaceutical, manufacturing and technology sectors.

Renato Leite Monteiro, Senior Associate, Opice Blum Law Firm

Renato specializes in Brazilian electronic law as a senior associate with Opice Blum Advogados, a law firm based in São Paulo, Brazil. He holds an LL.M. in Intellectual Property and Technology Law from New York University and the National University of Singapore (NUS). Other positions and memberships include: IP and Development Researcher of the NUS Centre for Law & Business; Editor of the Singapore Law Review; Council of Europe Expert on Privacy, Data Protection, Freedom of Speech and ICTs; Researcher of Center of Technology and Society of the Fundação Getúlio Vargas in Rio de Janeiro (FGV/RJ); Cyber Law Professor at Mackenzie University School of Law.

Gabriela Roitburd, Regional Compliance Counsel, Nokia Networks

Gabriela Roitburd is the head of Legal & Compliance for Mattel in Brazil. She has more than ten years of in-house experience in large multinational companies in the consumer, medical device, and pharmaceutical segments. This year she completes two, two-year terms as a member of the Ethics Committee of the Brazilian Association of High-Technology Industry of Medical Equipment, Products and Devices—ABIMED.

Weining Zou, Partner, Jun He Law Offices

Weining Zou is a partner of Jun He Law Offices. Zou joined Jun He in 1993 and currently practices out of the Beijing office. He has extensive experience in many areas relating to litigation and arbitration proceedings in China, and has successfully represented many multinational companies in complex commercial litigation, intellectual property, product liability and international trade.

ABOUT STEELE CIS

STEELE Compliance and Investigation Services (CIS) is a global business advisory and compliance intelligence firm offering comprehensive third-party due diligence solutions that help organizations comply with regulatory requirements and align with best practices. With more than 26 years of experience, STEELE CIS provides Fortune 1000 companies and mid-sized businesses with pragmatic solutions, including Regulatory Due Diligence, Third-Party Program Advisory Services, Program Management Services, and Compliance Analytics and Benchmarking Services. With engagements in more than 190 countries, STEELE CIS delivers local and regional expertise with 'on-the-ground' resources.

190+ COUNTRIES WITH STEELE ANALYSTS

To successfully mitigate corruption risk, you need to know more than just the language and customs. You need analysts and investigators who can skillfully navigate in-country intelligence and data privacy regulations. STEELE's professionals are this rare breed. More than 26 years of industry leadership and 1 million investigations translate into an unmatched third-party compliance program.

Let's talk about how to turn your compliance into confidence.

Call us today at **415-692-5000** or visit us at **www.steelecis.com**.

STEELE®
COMPLIANCE & INVESTIGATION SERVICES