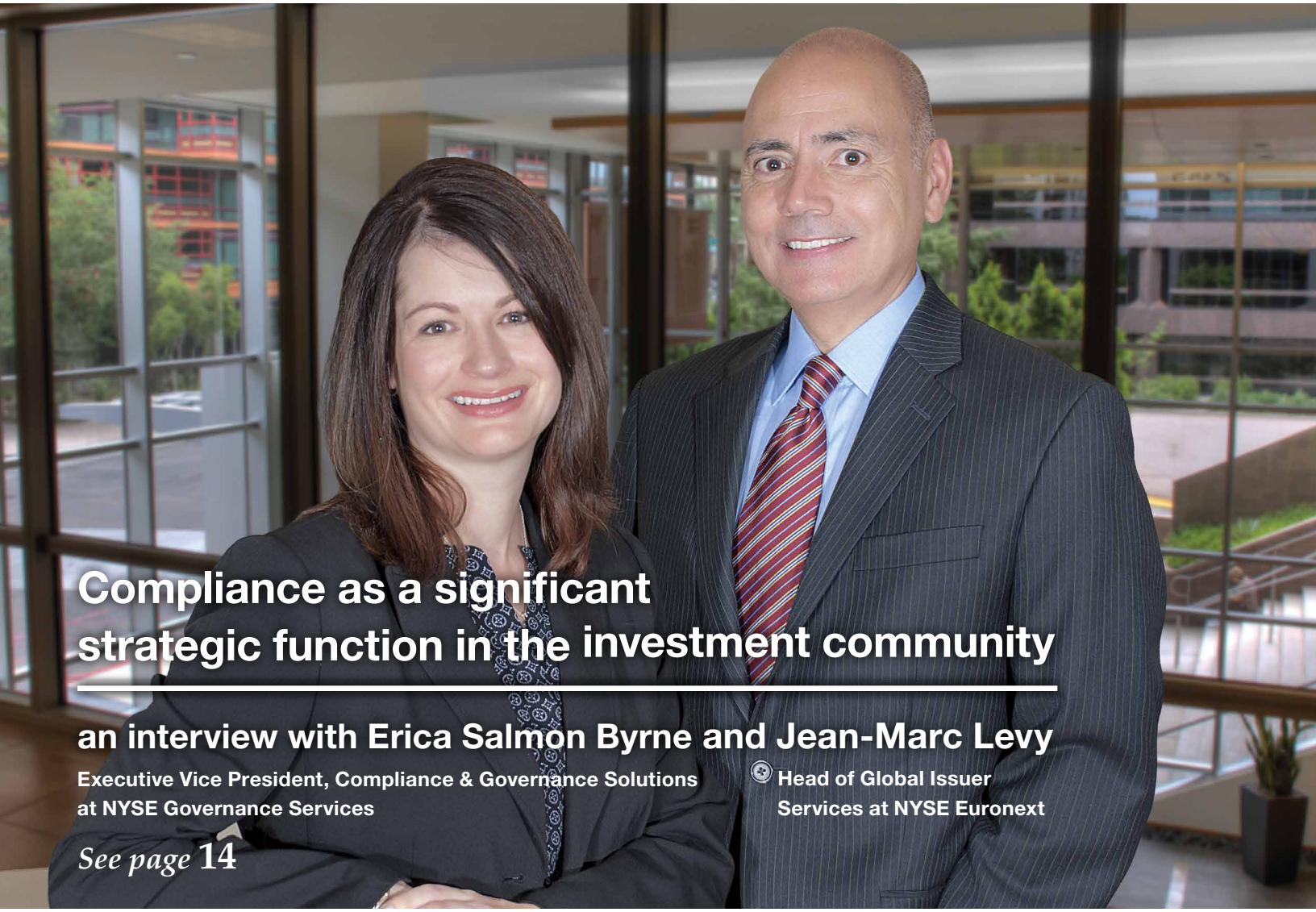
Compliance & Ethics Professional

November/December 2013

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

www.corporatecompliance.org



Compliance as a significant strategic function in the investment community

an interview with Erica Salmon Byrne and Jean-Marc Levy

Executive Vice President, Compliance & Governance Solutions at NYSE Governance Services

Head of Global Issuer Services at NYSE Euronext

See page 14

by Mónica Ramírez Chimal

Protection of personal data in private hands: Mexican privacy law

» Article 16 of the Constitution of the United Mexican States gives each person the right to privacy to protect information that is managed or accessed by individuals or legal entities.

» Companies should do a risk analysis of their processes to test their control mechanisms for mitigating the risks to which personal data is exposed.

» The Privacy Notice must be made according to several factors, including types of data that the company manages, how it is obtained, what is its purpose, etc.

» Companies should appoint someone to oversee compliance with the law and deal with the Federal Institute of Access to Information and Data Protection (IFAI), the authority in charge.

» The content of this law impacts the compliance with other laws, such as the Mexican Anti-Money Laundering Law.

On July 6, 2010, the Mexican Federal Law on the Protection of Personal Data in the Possession of Private Parties (the Privacy Law) was published. The regulations were issued on December 21, 2011, and went into effect in January 2012, giving people the authority to exercise their rights to data protection. Individuals who provide their services independently and legal entities (companies) who conduct the processing of personal data are subject to this law. The exceptions are:

Ramírez Chimal

- Information relating to companies;
- Information which refers to individuals as merchants and professionals; and
- The persons who provide services to any individual or legal entity with business activities and/or services consisting solely of its name, functions, or positions held, as well as some of the following data: work address, email, phone and fax number, if this information is treated for the purposes of representing the employer or contractor.

Also, on January 17, 2013 the Ministry of Economy issued Privacy Notice Guidelines for the content and scope of the privacy notice as well as good practices for using cookies, web beacons for tracking website visitors, or other automated means of gathering data. The Guidelines went into effect on April 17, 2013. The purpose of the law and its regulations is to protect personal data in order to ensure the privacy of persons. It defines personal data vs. sensitive personal data, the control mechanisms that companies must maintain, the responsibilities of those in charge, who owns the rights, and exceptions to the law, among others.

Definitions

"Personal data" means any information concerning an identified or identifiable person

such as name, phone number, address, photograph, fingerprints, and any other information that may identify the person.

"Sensitive personal data" are those that affect the most intimate sphere of the owner or involve a serious risk to privacy, such as racial or ethnic origin; health status; genetic information; religious, philosophical, and moral beliefs; union membership; public opinion; or sexual preference. Thus, the first mandatory step for companies is to determine what type of data is handled and who has access to it.

"Consent" is defined by law as the manifestation of the will of the owner. This means that the person agrees to give personal information. Depending on the data type, the consent will vary.

For personal data, consent is implied; express permission from the owner is not required. Such consent shall be considered accepted when the company shows the privacy notice to the owner and the owner does not express opposition.

For sensitive personal data, consent must be expressed in words that unambiguously demonstrate that permission has been granted. And this is mandatory when:

- required by law or regulation,
- financial or economic data are involved,
- requested by the company to accredit sensitive personal data, and/or
- the data owner and the company agree it is required.

Companies must manage a privacy notice, whether physical, electronic, audio, or any other format that is made available to the data holder or owner. The privacy notice must be given to the person prior to the collection of their information. The Privacy Notice Guidelines, issued in January 2013, differentiate three types of notice, depending on the way data is obtained:

- **Integral privacy notice:** applies when personal data is obtained from the owner personally, and this notice is the most complete.
- **Simplified privacy notice:** applies when personal data is obtained directly or indirectly from the owner. (It may be separate or integrated in the form.)
- **Short privacy notice:** applies when the space used for the collection of personal data is minimal and limited, so that the personal data collected or space for the dissemination of the privacy notice also is limited.

However, if the simplified or short version is used, companies are not exempt from providing the integral privacy notice so the data owner can verify it. That is, the company is required to prepare the integral privacy notice so it can be accessed by data holders/owners.

The integral privacy notice must contain:

- Company´s identity and address
- How the personal data and sensitive personal data will be treated
- Purpose for using the data
- Mechanism by which the owner may express his refusal prior to the processing of data
- How the company will handle data transfers, including nationally and internationally
- The mechanisms the data owners have to exercise their rights of access, rectification, cancellation, or opposition (ARCO)
- Mechanisms and procedures so that the owners may withdraw their consent
- Options and mechanisms that the company provides to the owner to limit the use or disclosure of data
- The means to limit the use, disclosure, or transfer of the data, including notice of and the opportunity to disable cookies

and/or web beacons before personal data is automatically collected; and
- Procedure and mechanisms by which the company will communicate to the owner any changes made to the privacy notice

The simplified privacy notice must contain:
- Company´s identity and address
- Purpose for collecting and using the data
- How to limit data use or disclosure
- How to exercise ARCO rights
- How to access the full integral privacy notice

The short privacy notice must contain only:
- Company´s identity and address
- Why the data is being collected
- How to access the full integral privacy notice

Steps for compliance

In addition to determining the types of data that the company manages, several points of analysis or review are required to meet both the requirements of law and regulation regarding the issuing of the privacy notice. First, companies should make an inventory of people/areas/companies, data, systems, and third parties who have access and/or manage data. Companies should make an elaborate flowchart of the information that shows how data moves, whether the data is in physical or electronic form, and where it is located (e.g., laptops, phones, server, etc.). This will help identify the controls that mitigate the risks of information leakage, destruction, alteration, transfer and data loss, unauthorized use or access; and any potential damages to the owner if the risks materialize.

Control measures for personal data cannot be lower than the ones the company uses for its own information. The law provides that in case of any vulnerability, the company should immediately inform the owner. Therefore, the risk analysis should consider the existence of vulnerabilities in the company or previous incidents.

Companies should make an elaborate flowchart of the information that shows how data moves, whether the data is in physical or electronic form, and where it is located (e.g., laptops, phones, server, etc.).

Second, make an inventory of the laws, rules, or regulations to which the company is subject. The law states exceptions to consent when personal data is covered under law, is from the public domain, is intended to comply with a legal relationship, or the person in charge has been outsourced by the company to a third party.

With the inventory of applicable laws, make a list of what is required for compliance with those laws. An example is the Federal Labor Law which in its Article 25 states that companies must generate a written working condition which includes: name, nationality, age, sex, marital status, Unique Key Population Register, Federal Register Taxpayers, and the worker's address. Therefore it is understood that such data are not subject to comply with the privacy law, but the company shall have sufficient mechanisms to show the reason why they are exceptions.

Third, once steps 1 and 2 have been done, companies must identify areas of opportunity and elaborate a work plan to help their controls minimize any identified risks. That is, for each control weakness or where there is any control, next steps will be determined

in order to protect personal data. The work plan is vital in the event that the authority audits a company; it will show that although there are weaknesses, they are being worked or improved.

The law states that companies should designate a person (either internally or externally) or an area responsible for processing personal data. If not performed internally, the functions of a third party should be documented by a contract that covers their existence, scope, and content. If the third party sub-hires, it must obtain authorization from the company. The exceptions are:

- in instances required by other law;
- transferring information to holding companies, subsidiaries, affiliates, or any associated company;
- when the transfer is necessary by virtue of a contract in the interest of the data owner between the company and a third party; and
- when the transfer is necessary for the maintenance or enforcement of a legal relationship between the company and the owner.

The person, area, or third party responsible for processing personal data must respond to requests from the rights holders for access, rectification, cancellation, and opposition of data. The potential ARCO scenarios are:

Access: The owner requests the company to state whether their databases have any of the owner's personal data.

Rectification: When the data is incorrect, incomplete, or outdated, the owner may request correction.

Cancellation: When data have already been used for the purpose or end for which it was requested, the company must eliminate or delete it. Or when the company fails to comply with the law and the owner requests to unsubscribe.

Opposition: When the owner does not want the company to continue to process or manage their data (e.g., for advertising or promotional purposes).

In this last case, the law states that the company is not required to remove personal data when:

- it refers to the content of a private contract, social or administrative agreement, and is necessary for its development and implementation;
- it should be treated by law;
- necessary to protect the interests of the owner; and
- necessary to comply with a legal obligation acquired by the owner.

Response times vary between 15 and 20 business days. If the company does not respond to the data owner´s request, he may exercise his right to the Federal Institute of Access to Information and Data Protection (IFAI), the responsible authority. IFAI may intervene between the owner and the company and/or carry out a review. The actions will depend on the nature of the complaint, if it is a recurrent problem, etc.

Fourth, companies must develop a policy and/or procedures, including the responsibilities of those who access or manage data, storage characteristics, response times to the owner and the authority, considerations for updating the policy and privacy notice, deletion of data, penalties for non-compliance, and training periods, among other topics.

Having conducted the analysis of information and issued internal rules, the company is ready to determine the purpose for which it requests the data, methods and mechanisms to limit the use or disclosure of data, and the methods and mechanisms for owners to

exercise their rights to ARCO, as well as to communicate changes to their acceptance of the privacy notice.

According to the activity of the company and data collection type, the privacy notice may be determined by what methods will be disclosed to the data owner.

In a final step, companies must include in their annual internal audit plan revisions to the controls that mitigate risks to personal data. At least once a year, companies must conduct training courses for staff on their responsibilities and the impact on the company that non-compliance may have.

Impact

Generically defined, the Privacy Law and its Guidelines mean companies face an interrelationship in both compliance controls and the Mexican Anti-Money Laundering Law.[1] In this respect, companies must conduct due diligence for employees, customers, and suppliers, as the Financial Action Task Force (FATF) indicates.[2]

When due diligence is performed on a customer or supplier, it does not mean that a contractual relationship will be established. Investigating the backgrounds of potential candidates to work in the company also does not form a contractual relationship. It's just a basic control measure to mitigate risks of fraud, mismanagement, and/or money laundering. In all these cases, companies should disclose the privacy notice in order to comply with the law.

In cases where the data is public, or when it is intended to comply with obligations under a legal relationship between the owner and the company, those are exceptions determined by law. That is, for customers, suppliers, and personnel who already work for the company, it is not necessary to obtain their consent, but it is a company´s responsibility to maintain confidentiality over their data and no risk to misuse of the data is disseminated.

The penalties that the Privacy Law and the Guidelines set by default depend on the nature and recurrence of the offense. Penalties can vary from 100 to 320,000 days of minimum wage in Mexico City[3] (approximately 6,476 to 20,723,200 pesos) and even prison for those responsible.

Generically defined, the Privacy Law and its Guidelines mean companies face an interrelationship in both compliance controls and the Mexican Anti-Money Laundering Law.

Conclusion

As noted, although the law requires an area, responsible person, or third party in charge of personal data and all the controls this entails, it really is a multidisciplinary exercise of all the company´s areas. A key success factor for the compliance with this law is to form a committee or group composed of representatives from the areas that own the controls that mitigate the risk of data protection and those areas in which personnel access and/or handle it. The company should also designate one person or area to consolidated feedback from the committee and to deal with the IFAI. The company must be completely sure that it is following the law and protecting the owner's data, as well as being ready for any revisions that might become law in the future. ✳

Mónica Ramírez Chimal *(mramirez@asserto.com.mx) is Partner Director of her own consultant firm, Asserto RSC in Mexico City.*

1. Ramirez Chimal: "New Mexican federal law to curtail money laundering." *Compliance & Ethics Professional*, July/August 2013, pp 65-69
2. FATF Recommendations issued in February 2012, indicate established control measures required for the recruitment of its employees. (Interpretative Note to Recommendation 18)
3. Minimum wage in the Federal District in January 2013 (and last issued) equals 64.76 pesos (about $5 a day).