A Timely Analysis of Legal Developments

ASAP®

July 29, 2013

Colombia Adopts Regulations to Implement its Data Protection Laws

By Geida Sanlate, Philip Gordon, Santiago Martinez Méndez, Juan Carlos Varela

With the advent of new rules regulating the protection of personal data, companies with operations in Colombia must implement policies and practices to comply with Colombia's privacy law. In October 2012, Colombia enacted Law 1581[1] to regulate the protection of personal data and safeguard the constitutional right of privacy in the midst of the challenges posed by globalization and new technologies that enable the easy electronic transfer of personal data. On June 27, 2013, Colombia's executive branch issued Decree 1377,[2] to implement various provisions of Law 1581. Decree 1377 went into effect immediately. This article discusses obligations arising under Law 1581 and Decree 1377, the steep potential sanctions for noncompliance, as well as recommendations for companies to ensure full compliance with the privacy law.

Law 1581 is part of a growing trend in Latin America to establish broad data protection regimes. As of this publication, Colombia joins Argentina, Costa Rica, Mexico, Peru and Uruguay in enacting such laws. Other countries in Latin America, such as Brazil, are considering similar legislation. U.S. multinationals with employees in Latin America should closely follow this trend.

The Constitutional Right of Privacy

Under the Political Constitution of Colombia of 1991, all citizens have an inviolate fundamental right to personal and familial privacy and to the protection of their good name. Until the enactment of Law 1581, Colombia's constitutional courts interpreted and enforced this right of privacy. However, companies were left to interpret the scope of these decisions when attempting to comply with the law.

In an apparent attempt to create a uniform legal framework for the protection of personal data, Law 1581 codifies the precedential judicial decisions on this topic and further imposes extensive requirements to ensure that public and private entities collecting, processing and/or transferring personal data do so without compromising citizens' privacy rights. Law 1581 also makes it clear that the right to access, correct and challenge the use of personal data extends to every person, regardless of age or gender, and every area of society, including the workplace.

1 Law 1581, entitled "General Provisions for the Protection of Personal Data", was promulgated into law on October 17, 2012.

2 Decree 1377 ("Decreto 1377 de 2013") was issued by Colombia's Superintendencia de Industria y Comercio (Superintendency of Industry and Commerce or "SIC") on June 27, 2013.

Important Provisions of the Privacy Law

The privacy law imposes various obligations on any "responsible party" that directly or indirectly processes personal data about the data owner. Law 1581 defines the "responsible party" as the public or private individual or entity that processes the personal data or decides how the data should be processed or the database safeguarded. The data owner is the individual whose personal data is processed. The processing of personal data encompasses the collection, processing, storage, use, transfer or suppression of any information that can be associated with an identified or identifiable individual.

Since employers, as part of their normal course of business, typically collect and process the personal data of their prospective, current or former employees, employers should be especially mindful of the following important provisions under the law:

Privacy notice. Either in writing, verbally or electronically, the responsible party must notify the data owner about: (i) the purpose driving the data collection or processing; (ii) the intended use of the personal data; (iii) the data owner's privacy rights; and (iv) how the data owner can access the responsible party's policies that regulate the processing of personal data. To avoid any contention that an employee received, but did not understand, the notice, we recommend that the privacy notice be made in Spanish and in simple, clear and understandable language.

Consent requirements (generally). The responsible party must obtain the data owner's unequivocal consent prior to processing the personal data. As such, for the consent to be valid, it must be accompanied by a privacy notice that contains all of the information described above. The consent must be expressly stated and can be provided in writing, verbally, or through methods that would advise the responsible party that the data owner has expressly consented to the processing of his or her personal information. However, in no way can silence be deemed as consent. We recommend that, where possible, the employer obtain a signed consent, to be able to establish the data owner's express consent.

The law requires the responsible party preserve proof of the data owner's unequivocal consent. Concerning this recordkeeping requirement, the privacy law is unclear as to the length of time that a responsible party is required to preserve the proof of consent. Nonetheless, it would be prudent for employers to implement procedures whereby data owners provide unequivocal consent, as well as to retain proof of such consent for at least 3 years from the date the employment relationship ends, so as to align it with statute of limitations period for any employment-related claim.

Consent can be revoked at any time, except that such revocation will be deemed invalid if it is made to avoid a legal or contractual obligation. At all times, the responsible party must provide a procedure for the data owner to revoke the consent easily and at no charge. If the processing of the personal data exceeds the purpose for which it was collected, the data owner shall have the right to petition the Superintendency of Industry and Commerce ("SIC"), the regulatory agency in charge of enforcing this law, to order the revocation or suppression of the personal data.

Consent for processing and protection of sensitive personal data. Except in limited circumstances, processing of sensitive personal data is prohibited. Sensitive personal data refers to information intimately tied to the data owner's personal characteristics, such as race, ethnicity, medical condition, sexuality, political association, religious or philosophical beliefs, membership in a union or human rights organization or biological data. Because such data can be improperly used to discriminate against individuals, the privacy law provides that no action or activity can be made contingent upon the data owner providing his or her sensitive personal data for processing. This means that an employer is not allowed to require that a current or prospective employee provide his or her sensitive personal data for hiring or continued employment, unless the employer is required by law to collect this information, as it is in the case, for example, where a current or prospective employee is required to undergo a medical exam for a legitimate business reason.

Assuming the collection or processing of the sensitive personal data is allowed, the responsible party nonetheless must ensure that the data is adequately protected and kept confidential.

Processing or use of personal data is limited to specific time and objective. Even with the data owner's consent, the responsible party can process the personal data only for a limited time and consistent with the purpose for which the data was collected. Once the objectives of the processing have been fulfilled, the responsible party is required to suppress the personal data, unless such data must be maintained to comply with a legal, contractual or administrative obligation. With this language, there is a legitimate argument that the privacy law allows employers to preserve and access the personal data of current and former employees for as long as it is required to comply with myriad of obligations arising after a termination or relative to the social security laws.

International and other types of transfer of personal data. Whenever the responsible party transfers personal data to a third party, such as a data processor (for example, an employer that transfers personal data to a vendor for purposes of conducting a background check), the responsible party must enter into an agreement where the third party agrees to process the personal data only for the purposes for which the personal data was collected. This means that, in no way can the personal data be processed for any other purpose without the data owner's express consent.

The law is stringent regarding international transfers of personal data, such as when a subsidiary corporation located in Colombia transfers personal data to its parent corporation in the U.S. In such cases, the transfer is prohibited, unless the personal data will be transferred to a country with equal or higher standards for the adequate protection of personal data than those required by Law 1581. This prohibition does not apply where the SIC has determined that the third country provides an adequate level of protection or when the transfer has been made in accordance with an international treaty to which Colombia is a signatory. As of this writing, no guidance has been provided as to whether Colombia will recognize the U.S.-E.U. Safe Harbor Framework as meeting the adequacy standard.

This prohibition notwithstanding, the privacy law provides various exceptions to the adequacy requirement. Two potentially relevant exceptions for employers are (a) when the data owner has provided his or her express and unequivocal consent to the transfer, and (b) where the transfer is necessary for the fulfillment of a legal or contractual obligation.

Internal policies available to data owner. The responsible party must establish and implement policies and methods to adequately protect the privacy and confidentiality of the personal data. It is recommended that employers adopt policies that provide guidance to human resources and IT employees on the proper handling of personal data.

Enforcement and sanctions for noncompliance. Decree 1377 establishes that the Superintendency of Industry and Commerce is authorized to enforce Law 1581 and impose sanctions for non-compliance. Specifically, the SIC may impose a fine in the amount of 2,000 times the general minimum salary in effect at the time of the fine. At the time of this publication, the maximum fine would amount to US $627,411. Other sanctions that may be imposed include suspension of operations for up to six months, a temporary (but indefinite) shut down of operations if the company has not corrected its practices to fully comply with the law, or permanent closure of operations if the company refuses to comply with its obligations under the law.

Recommendations

In promulgating the new privacy law, Colombia has joined the international community of countries that have enacted laws for the adequate protection of personal data. With a new legal framework, data owners now enjoy greater protections of their personal information, and individuals and entities are now required to comply with new and extensive obligations with regards to the collection, use and processing of personal data. We believe that this is only the beginning as Colombia's executive branch has announced its commitment to protect the right of privacy in a fast evolving technological age.

Because the privacy law applies at a national level, all individuals or entities that furnish or process personal data within the territory of Colombia are covered, unless specifically exempted under the law. Therefore, employers must comply with the privacy law when collecting or processing personal data and to transfer it outside of Colombian borders. For example, a parent corporation that collects personal data in Colombia to process it in another country should ensure that the data owner has provided express and unequivocal consent to such international transfer.

It is expected that the SIC will conduct inspections to monitor compliance, placing special focus on the health and financial industries, given these industries' reliance on collecting and processing personal data to conduct their activities. Domestic and multinational employers should nonetheless take the necessary measures to ensure full compliance. As part of such measures, we recommend that companies adopt these additional measures:

1. Create and implement internal policies to regulate the proper treatment and adequate protection of personal data, whether it relates to the collection, processing, storage, use, transfer or deletion of such data. Such measures should aim to ensure that no sensitive personal data is ever made public.
2. Communicate such policies in a uniform manner to all current employees authorized to process personal data and obtain their acknowledgement of receipt.
3. Identify the specific purpose for which the personal data may be processed.
4. Provide a privacy notice to job applicants and current employees, detailing the key information discussed above, as well as explaining whether the data will be used for purposes other than complying with a legal or contractual obligation.
5. Obtain the data owner's express and unequivocal consent to the processing of the personal data. Preserve proof of (i) the data owner's express and unequivocal consent to the personal data processing, and (ii) the acknowledgement of receipt of the privacy notice.
6. Process the personal data only for the purposes for which it was collected as stated in the privacy notice.
7. Prior to transferring any personal data to a third-party service provider, ensure that the service provider has agreed, by contract, to protect it in accordance with your company's policies and to process the personal data consistent with the objective for which it was collected.
8. Since the processing or use of personal data is limited to a time or a specific purpose, employers holding personal data of former employees should abstain from processing or using it for any purpose inconsistent with those stated in the privacy notice.
9. Obtain a signed agreement of confidentiality from employees handling confidential personal data. This agreement should be included as part of the employment contract, where the parties will agree that a breach of the confidentiality agreement will be just cause for termination.

Finally, as several of the above steps emphasize, it is critical that employers meticulously document each step of the process. Taking on all of these measures will be irrelevant if at the time of an SIC inspection the employer is unable to prove compliance. Employers should seek legal counsel from experts in this field, with proven experience in helping domestic employers and multinational companies, to comply with Colombia's privacy law.

Philip Gordon is a shareholder of Littler Mendelson's office in Denver, Colorado and the Chair of Littler's Privacy and Data Protection Practice Group. Juan Carlos Varela is the Office Managing Shareholder of Littler's office in Caracas, Venezuela and Co-Chair of Littler's Latin America Practice Group. Geida Sanlate is an attorney in Littler's Knowledge Management department, with special focus on international employment laws. Special thanks to Santiago Martinez Méndez, Senior Attorney and leader of the Audit and Corporate Compliance Practice Group in the law firm of Godoy, Córdoba Abogados, S.A.S., in Bogota, Colombia, for his important contributions to this article. If you would like further information, please contact Mr. Gordon at pgordon@littler.com or 303.362.2858; Mr. Varela at jcvarela@littler.com or 305.400.7590; Ms. Sanlate at gsanlate@litter.com or 973.848.4744; or Mr. Martinez Mendez at smartinez@godoycordoba.com or 57.571.317.4628. For information concerning the Godoy Cordoba law firm, please visit their website at www.godoycordoba.com. For information concerning Littler, please visit their website at www.littler.com.