 © Copyright Lex Mundi Ltd. 2012

DATA PRIVACY

COLOMBIA
Brigard & Urrutia Abogados

CONTACT INFORMATION
Juliana Pulecio Velásquez
Brigard & Urrutia Abogados
Calle 70 A #4-41
Bogotá, Colombia
571 346 2011 Ext. 8771
jpulecio@bu.com.co

1. Provide a brief description of the subject matter of data privacy laws in your jurisdiction that are applicable to Personally Identifiable Information, and any material obligations.

a) What is the cite to such laws? Provide a link, if available, to an online copy of such law.

On December, 2010, Colombian Congress enacted a new general data protection law (the "New Data Protection Act" or "NDPA") which established the regulations for processing personal information. As this law regulates fundamental rights, it required the prior approval by the Constitutional Court to enter into force. Although the Court´s decision is not yet public, on a recent press release the Court established that with the exception of a few articles the NDPA passed the constitutional test.

http://www.oas.org/dil/Newsletter/newsletter_api_ppd_NOV-2011_Colombia_new_law.pdf

b) What are the penalties imposed for a breach of such law? Any criminal sanctions?

The Superintendency of Industry and Commerce (The Colombian data privacy authority)

may impose the following sanctions for non-compliance of the NDPA: (i) fines up to USD 596.500, (ii) suspension of activities related to the processing and/or (iii) permanent or temporary closure of the operation.

In addition, pursuant to Law 1273 of 2009, it is a crime to "obtain, gather, subtract, offer, sell, exchange, send, buy, intercept, divulge, modify or use personal data (…) for personal purposes or of third parties, without being authorized to do so". Individuals or companies that commit this crime may be subject to fines of up to USD 220,000, and prison of 4 to 8 years.

c) Identity the applicable administrative authority with jurisdiction for enforcement of such laws.

Superintendency of Industry and Commerce.

d) Any additional information that is material?

2. Provide a brief description of the subject matter of data privacy laws in your jurisdiction that are applicable to Personal Health Information, and any material obligations.

a) What is the cite to such laws? Provide a link, if available, to an online copy of such law.

Although there are some specific provisions in the Colombian health care regulations regarding the processing of personal health information, as the NDPA is not yet enforceable, the rules for the processing of such information when considered personal data have been established by the judicial precedents of the Constitutional Court.

The Constitutional Court has defined personal information as any information that by itself or in connection with other information may identify a particular individual. The Court has issued about 200 decisions since 1991 in connection with three fundamental rights that have direct impact on the protection of personal information: the habeas data right, the right to privacy, and the right to maintain a public good name. One of these decisions, decision T–729 of 2002 ("Decision T-729"), is one of the landmark decisions in connection with the right to personal data protection. This decision sets forth the principles for the processing of personal data, of which it is important to mention the following:

Freedom: Personal Data can only be processed with the free, express, informed, and prior consent of the data subject.

Purpose: The Personal Data collected must have an explicit, determined and legitimate purpose. This purpose must be informed to the data subject and its Processing must be carried out within the scope of the notified purpose.

Restricted circulation: The Personal Data collected may only be circulated within the parameters of the freedom and purpose principles. Therefore, the Personal Data may only circulate within the legal entity that has legitimately obtained such information and the people expressly authorized by the data subject. Any transfer to third parties, even if affiliated, must be previously authorized by the data subject.

Necessity: Only the specific Personal Data that is required for the authorized purpose may be collected. Conversely, no information that is not specifically required for the authorized purpose may be collected.

Veracity or quality of the data: Personal Data stored in databases must be true, complete, exact, up to date, verifiable and comprehensible. Recording of information that is partial, incomplete, fragmented or that induces to error is forbidden.

Temporality: Personal Data must only be stored as long as it is useful for the authorized purpose for which it was collected.

Security: Personal Information shall be handled using the necessary technical measures that guarantee its safety and integrity of the records as a whole.

Confidentiality: All individuals and legal entities that intervene in the administration of Personal Data shall guarantee at all times the confidentiality of such information, even after they cease their labors.

b) What are the penalties imposed for a breach of such law? Any criminal sanctions?

As the NDPA is not currently enforceable there are no specific penalties for violation of the principles set forth by the Constitutional Court. Therefore, risks must be evaluated on a case by case basis.

c) Identity the applicable administrative authority with jurisdiction for enforcement of such laws.

Superintendency of Industry and Commerce and the Ministry of Health and Social Protection without being authorized to do so.

d) Any additional information that is material?

3. Provide a brief description of the subject matter of data privacy laws in your jurisdiction that are applicable to Financial Information, and any material obligations.

 © Copyright Lex Mundi Ltd. 2012

a) What is the cite to such laws? Provide a link, if available, to an online copy of such law.

Law 1266 of 2008 ("Financial data Privacy Act"). This law was originally intended to be the general legal framework applicable to the management of personal information. However, after being reviewed by the Constitutional Court (Decision C 1011 of 2008), its scope was reduced to be applicable only to financial, credit, commercial, and services information (and to information of the same characteristics coming from abroad) destined to financial risk and credit risk assessment ("Financial Personal Data"). The paradigm case to which Law 1266 is applied would be the data collected by financial institutions to determine whether or not they would grant a loan to their clients. However, the Court has sustained that this Law 1266 applies to all data used by people other than financial institutions with the purpose of analyzing credit risk.

http://www.secretariasenado.gov.co/senado/basedoc/ley/2008/ley_1266_2008.html

b) What are the penalties imposed for a breach of such law? Any criminal sanctions?

According to the Financial Data Privacy Act, the Superintendency of Finance may impose the following sanctions for non-compliance of the Financial Data Privacy Act: (i) fines up to USD 447.395, (ii) suspension of activities related to the data base administrator and/or (iii) permanent or temporary closure of the activities related to the management of the data base.

In addition, pursuant to Law 1273 of 2009, it is a crime to "obtain, gather, subtract, offer, sell, exchange, send, buy, intercept, divulge, modify or use personal data (…) for personal purposes or of third parties, without being authorized to do so". Individuals or companies that commit this crime may be subject to fines of up to USD 220,000, and prison of 4 to 8 years.

c) Identity the applicable administrative authority with jurisdiction for enforcement of such laws.

The Superintendency of Finance.

d) Any additional information that is material?

 © Copyright Lex Mundi Ltd. 2012

4. Provide a brief description of the subject matter of data privacy laws in your jurisdiction that is applicable to other sensitive data, and any material obligations.

a) What is the cite to such laws? Provide a link, if available, to an online copy of such law.

Pursuant to the NDPA, processing of sensitive data, understood as any data that affects the privacy of the data subject or which its unlawful use may cause that the data subject could be discriminated, is generally prohibited unless expressly authorized by law or if the data subject has granted its explicit consent for such processing. Data subject has the right to refuse providing any information regarding sensitive data.

b) What are the penalties imposed for a breach of such law? Any criminal sanctions?

Please see section 1b.

c) Identity the applicable administrative authority with jurisdiction for enforcement of such laws.

d) Any additional information that is material?