In this third article of a four-part series on the status of data protection laws, the author explores developments in the Western Hemisphere (Latin America, the Caribbean, and Canada), where 15 jurisdictions now have comprehensive data protection laws.

**Western Hemisphere Data Privacy Laws in the Western Hemisphere (Latin America, Caribbean and Canada)**

*By Cynthia Rich*

**Introduction and Region at-a-Glance**

Fifteen jurisdictions in the Western Hemisphere (Latin America, Caribbean, and Canada) now have comprehensive privacy laws including: Antigua and Barbuda, Argentina, Aruba, Bahamas, Bolivia, Canada, Chile, Colombia, Costa Rica, Curacao, Dominican Republic, Ecuador, El Salvador, Guatemala, Guyana, Haiti, Honduras, Nicaragua, Panama, and Paraguay. Saint Lucia adopted legislation in 2011, but the law hasn’t yet gone into effect. The laws in Argentina, Canada and Uruguay (12 WDPR 16, 9/21/12) have been deemed by the European Commission to provide adequate protection.

Other countries such as Bermuda, Brazil (16 WDPR 05, 5/26/16), Ecuador, Jamaica, and Panama, and territories such as Puerto Rico, have also enacted data protection laws. The laws in Argentina, Canada, and Uruguay (12 WDPR 16, 9/21/12) have been deemed by the European Commission to provide adequate protection.
This article examines the commonalities and differences among the privacy laws in the region and discusses current trends and new developments.

Common Elements Found in Latin American Laws

All of the laws in the region include some type of notice obligation. That is, every law requires that individuals be told what personal information is collected, when it is collected and with whom it is shared.

Choice:

Every privacy law also includes some type of choice obligation. This level of type of consent varies significantly from country to country. Argentinians, for example, specify that personal information must be collected only for the purpose for which it is collected and that individual’s must be informed before the data is transferred to another country. In contrast, other countries have provisions that are somewhat similar, but do not include such a clear statement.

Security:

While core data protection principles and requirements are embodied in all of these laws, specific requirements, such as data breach notification, data security, data retention, and DPO obligations, vary widely from country to country. In addition, some laws require registration and notification in the event of a data breach and one-quarter require the appointment of a data protection officer (DPO). Some of the DPAs in the region do not provide adequate protection, thus, organizations are left to assume that all countries are adequate in protecting personal information.

Access and Correction:

While core data protection principles and requirements are embodied in all of these laws, the regions’ approaches to access and correction requests in a much shorter period of time. Differences in Approaches.

While every data protection principle and requirement is included in all of these laws, specific requirements, such as data breach notification, data security, data retention, and DPO obligations, vary widely from country to country. In addition, some laws require registration and notification in the event of a data breach and one-quarter require the appointment of a data protection officer (DPO). Some of the DPAs in the region do not provide adequate protection, thus, organizations are left to assume that all countries are adequate in protecting personal information.

Notice:

All of the laws in the region include some type of notice obligation. That is, every law requires that individuals be told what personal information is collected, when it is collected and with whom it is shared.

Choice:

Every privacy law also includes some type of choice obligation. This level of type of consent varies significantly from country to country. Argentinians, for example, specify that personal information must be collected only for the purpose for which it is collected and that individual’s must be informed before the data is transferred to another country. In contrast, other countries have provisions that are somewhat similar, but do not include such a clear statement.

Security:

While core data protection principles and requirements are embodied in all of these laws, specific requirements, such as data breach notification, data security, data retention, and DPO obligations, vary widely from country to country. In addition, some laws require registration and notification in the event of a data breach and one-quarter require the appointment of a data protection officer (DPO). Some of the DPAs in the region do not provide adequate protection, thus, organizations are left to assume that all countries are adequate in protecting personal information.

Access and Correction:

While core data protection principles and requirements are embodied in all of these laws, the regions’ approaches to access and correction requests in a much shorter period of time.
suits and government enforcement actions are actively imposing significant penalties for privacy violations. For example, in September 2015, the DPA announced its plans to impose a fine of approximately $78,600 for publishing sensitive personal information of two citizens on its website. The Peruvian DPA fined the Peruvian company datospe with $50,000 for privacy law violations involving the use of sensitive personal information for marketing purposes without the individual's consent. In 2014, the Colombian DPA fined a shopping mall $22,503 for violating its notice obligations. In addition, a chart is provided at the end to show the countries with mandatory cross-border transfers, some of which have been quite high.

Of all of the authorities in the region, the Data Protection Authorities in Mexico has been the most active in issuing fines, some of which have been quite high.

Privacy Legislation Under Development
Several jurisdictions in the region that do have laws in place are currently developing legislation. These include Colombia, Brazil, and the Cayman Islands. During its public consultation in July 2015, the Brazilian government submitted a draft model law which, in addition to the basic obligations of protection, would impose a complex and burdensome set of rules on organizations that collect, maintain or store data from Brazilian consumers.

Privacy staffing requirements. Compliance programs that comply with all the requirements of the law and those that comply with only European Union and Asian obligations will run afoul of many of the country obligations in this region. A country-by-country summary of the obligations in these laws is provided below. Other noteworthy characteristics are also highlighted and, where applicable, the responsible enforcement authority is indicated. To provide a glance at the countries with mandatory cross-border transfers, some of which have been quite high. For example, in September 2015, the DPA announced its plans to impose a fine of approximately $78,600 for publishing sensitive personal information of two citizens on its website. The Peruvian DPA (approximately $78,600) for publishing sensitive personal information of two citizens on its website. The Peruvian DPA imposed a fine of $50,000 for privacy law violations involving the use of sensitive personal information for marketing purposes without the individual's consent. In 2014, the Colombian DPA imposed a fine of approximately $78,600 for publishing sensitive personal information of two citizens on its website. The Peruvian DPA ($22,503) for violating its notice obligations. In addition, a chart is provided at the end to show the countries with mandatory cross-border transfers, some of which have been quite high.

Of all of the authorities in the region, the Data Protection Authorities in Mexico has been the most active in issuing fines, some of which have been quite high.

Privacy Legislation Under Development
Several jurisdictions in the region that do have laws in place are currently developing legislation. These include Colombia, Brazil, and the Cayman Islands. During its public consultation in July 2015, the Brazilian government submitted a draft model law which, in addition to the basic obligations of protection, would impose a complex and burdensome set of rules on organizations that collect, maintain or store data from Brazilian consumers.

Privacy staffing requirements. Compliance programs that comply with all the requirements of the law and those that comply with only European Union and Asian obligations will run afoul of many of the country obligations in this region. A country-by-country summary of the obligations in these laws is provided below. Other noteworthy characteristics are also highlighted and, where applicable, the responsible enforcement authority is indicated. To provide a glance at the countries with mandatory cross-border transfers, some of which have been quite high. For example, in September 2015, the DPA announced its plans to impose a fine of approximately $78,600 for publishing sensitive personal information of two citizens on its website. The Peruvian DPA imposed a fine of $50,000 for privacy law violations involving the use of sensitive personal information for marketing purposes without the individual's consent. In 2014, the Colombian DPA imposed a fine of $22,503 for violating its notice obligations. In addition, a chart is provided at the end to show the countries with mandatory cross-border transfers, some of which have been quite high.
countries. Moreover, the proposed law would expand the categories of personal data sensitive to countries. In addition, the Privacy Commissioner was given additional powers to enter into a compliance agreement with an organization if the Commissioner reasonably believes that the organization has committed, or is likely to commit, a breach of PIPEDA.

Lastly, in Mexico, there are plans to introduce a privacy bill in 2016 that combines regulations over the public and private sector. According to an article in Mexico’s renovation of the Federal Law of Access to Information and Transparency (Ley de Transparencia, Accesibilidad e Información, or LTAI), there is a bill being introduced this year that would make it easier for individuals to be able to access data from one company to the other, strengthen data protection rules, and provide for additional measures to protect personal data.

The Antigua and Barbuda Law does not require data breach notification and requires the regulator to be notified about data breaches. Individuals would have to be given immediate notice of a data breach involving their personal information and the regulator to be notified about data breaches. In-Country Review of Differences

ANTIGUA AND BARBUDA

The Data Protection Act (Antigua and Barbuda Law), enacted in 2016, protects personal data processed by public and private sector organizations.

In Brief:

The Antigua and Barbuda Law does not require database registration, data security breach, or data breach notification, or employee privacy rules (e.g., prohibit “excessive monitoring” of employees).

Special Characteristics

Data Protection Authority

The Information Commissioner is the regulator who enforces the provisions of the Antigua and Barbuda Law. There is no web site available for the Information Commissioner.

Compliance

Compliance is required to process personal data within an organization. By agreement, the Commissioner has the right to conduct inspections of organizations to ensure compliance with applicable laws. There is no specific enforcement authority to enter into a compliance agreement with an organization if the Commissioner reasonably believes that the organization has committed, or is likely to commit, a breach of the Act.

Definition of Personal Data

Personal data are defined as any information processed in the context of “commercial transactions.” Such commercial transactions include, but are not limited to, transactions involving credit cards, insurance, and the provision of goods or services, whether contractual or not, in the context of “commercial transactions.” Such commercial transactions involve business activities, but do not include any matter relating to the supply or exchange of goods or services on an arm’s-length basis, and any matters relating to the supply or exchange of goods or services on a non-commercial basis.

Consent

Consent is required to process personal data unless an exception applies (e.g., contractual necessity, legal obligation). Explicit consent is required to process sensitive personal data.

In Canada, Chile, Costa Rica and Mexico that are working on amending their existing privacy laws, there are also countries in the region such as Canada, Chile, Costa Rica and Mexico that are working on amending their existing privacy laws. Late in 2014, the State Minister for Science, Technology, Energy and Mining announced in November that a draft Data Protection Act is being circulated for review and comment by key stakeholders and the bill is expected to be tabled in Parliament by the end of 2015 legislative year.

Amendments to Existing Privacy Laws

There are also countries in the region such as Canada, Chile, Costa Rica and Mexico that are working on amending their existing privacy laws. In late 2014, the State Minister for Science, Technology, Energy and Mining announced in November that a draft Data Protection Act is being circulated for review and comment by key stakeholders and the bill is expected to be tabled in Parliament by the end of 2015 legislative year.

Amendments to Existing Privacy Laws

There are also countries in the region such as Canada, Chile, Costa Rica and Mexico that are working on amending their existing privacy laws. In late 2014, the State Minister for Science, Technology, Energy and Mining announced in November that a draft Data Protection Act is being circulated for review and comment by key stakeholders and the bill is expected to be tabled in Parliament by the end of 2015 legislative year.

Amendments to Existing Privacy Laws

There are also countries in the region such as Canada, Chile, Costa Rica and Mexico that are working on amending their existing privacy laws. In late 2014, the State Minister for Science, Technology, Energy and Mining announced in November that a draft Data Protection Act is being circulated for review and comment by key stakeholders and the bill is expected to be tabled in Parliament by the end of 2015 legislative year.

Amendments to Existing Privacy Laws

There are also countries in the region such as Canada, Chile, Costa Rica and Mexico that are working on amending their existing privacy laws. In late 2014, the State Minister for Science, Technology, Energy and Mining announced in November that a draft Data Protection Act is being circulated for review and comment by key stakeholders and the bill is expected to be tabled in Parliament by the end of 2015 legislative year.

Amendments to Existing Privacy Laws

There are also countries in the region such as Canada, Chile, Costa Rica and Mexico that are working on amending their existing privacy laws. In late 2014, the State Minister for Science, Technology, Energy and Mining announced in November that a draft Data Protection Act is being circulated for review and comment by key stakeholders and the bill is expected to be tabled in Parliament by the end of 2015 legislative year.

Amendments to Existing Privacy Laws

There are also countries in the region such as Canada, Chile, Costa Rica and Mexico that are working on amending their existing privacy laws. In late 2014, the State Minister for Science, Technology, Energy and Mining announced in November that a draft Data Protection Act is being circulated for review and comment by key stakeholders and the bill is expected to be tabled in Parliament by the end of 2015 legislative year.

Amendments to Existing Privacy Laws

There are also countries in the region such as Canada, Chile, Costa Rica and Mexico that are working on amending their existing privacy laws. In late 2014, the State Minister for Science, Technology, Energy and Mining announced in November that a draft Data Protection Act is being circulated for review and comment by key stakeholders and the bill is expected to be tabled in Parliament by the end of 2015 legislative year.

Amendments to Existing Privacy Laws

There are also countries in the region such as Canada, Chile, Costa Rica and Mexico that are working on amending their existing privacy laws. In late 2014, the State Minister for Science, Technology, Energy and Mining announced in November that a draft Data Protection Act is being circulated for review and comment by key stakeholders and the bill is expected to be tabled in Parliament by the end of 2015 legislative year.
**Western Hemisphere Privacy Laws**

<table>
<thead>
<tr>
<th>Country or Region</th>
<th>Registration Requirement</th>
<th>Data Security Breach Notification Requirement</th>
<th>Cross-Border Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antigua &amp; Barbuda</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Argentina</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Australia</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Bahamas</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Barbados</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Belize</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Bolivia</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Brazil</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Canada</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Chile</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Colombia</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Costa Rica</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Curacao</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Dominica Republic</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Dominica</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>El Salvador</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Falkland Islands</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>France</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Georgia</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Greece</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Greenland</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Guatemala</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Haiti</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Honduras</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Jamaica</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Japan</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Jordan</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Malaysia</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Mexico</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Mongolia</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Morocco</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Panama</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Paraguay</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Peru</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Puerto Rico</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Saint Vincent</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Suriname</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Trinidad &amp; Tobago</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Uruguay</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Venezuela</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Western Hemisphere (35)</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

1. In some jurisdictions, the appointment of a DPO may exempt the organization from its registration obligations.
2. This chart is based on currently existing laws and regulations or pending legislation. It does not reflect the local notification procedures of the DPA’s expectations about whether organizations should consider a security breach notification service. Consequently, organizations should consider a variety of factors, not just whether the rules are legally binding.

To Brief

The Argentine Data Protection Act (Argentine Law (in Spanish)), enacted in 2000, protects all personal information of natural persons (living and deceased) and legal entities recorded in public or private data files, registers and data banks, established for the purpose of providing reports. Argentina was the first country, and currently only one of two countries in Latin America, to be recognized by the European Union as providing an adequate level of protection for personal information transferred from the EU/European Economic Area to third countries.

**Special Characteristics**

**Data Protection Authority**

The National Directorate for Personal Data Protection, located under the Justice and Human Rights Ministry, is responsible for enforcement of the Argentine Law.
Cross-Border Transfers

The Aruba Law prohibits transfers of personal information into the files to which the Law isn’t applicable. In the event of a data security breach, the DPA requires the data controller to provide the DPA with appropriate contract in place. The DPA has appended specific clauses that it will use as a parameter for assessing international transfers agreements.

Registration

The Aruba Law imposes restrictions on cross-border transfers but doesn’t require database registration, the establishment of a DPO or data security breach notification.

 Notice and Consent

While there are no explicit notice and consent requirements set forth in the Aruba Law, the DPA encourages the obligation to collect and process personal information only from those individuals that individually must be made aware of certain information regarding the processing of their personal information and that process information that is required to be sent to or processed in third countries.

In Brief

The Aruba Law imposes restrictions on cross-border transfers but doesn’t require database registration, the establishment of a DPO or data security breach notification.

Special Characteristics

Data Protection Authority

The Office of the Data Protection Commissioner is responsible for investigating any contraventions of the Bahamas Law, either of its own volition or as a result of a complaint by an individual concerned.

Notice and Consent

While there are no explicit notice and consent requirements set forth in the Bahamas Law, the DPA encourages the obligation to collect and process personal information only from those individuals that individually must be made aware of certain information regarding the processing of their personal information and that process information that is required to be sent to or processed in third countries.

Data Protection Authority

The Office of the Data Protection Commissioner is responsible for investigating any contraventions of the Bahamas Law, either of its own volition or as a result of a complaint by an individual concerned.

Consent is not required to transfer in a secure manner to an appropriate country, provided that it is an appropriate manner to use the data.

The Aruba Law imposes restrictions on cross-border transfers but doesn’t require database registration, the appointment of a DPO or data security breach notification.

Cross-Border Transfers

The Aruba Law prohibits transfers of personal information into the files to which the Law isn’t applicable. In the event of a data security breach, the DPA requires the data controller to provide the DPA with appropriate contract in place. The DPA has appended specific clauses that it will use as a parameter for assessing international transfers agreements.

Registration

The Aruba Law imposes restrictions on cross-border transfers but doesn’t require database registration, the establishment of a DPO or data security breach notification.

 Notice and Consent

While there are no explicit notice and consent requirements set forth in the Aruba Law, the DPA encourages the obligation to collect and process personal information only from those individuals that individually must be made aware of certain information regarding the processing of their personal information and that process information that is required to be sent to or processed in third countries.

In Brief

The Aruba Law imposes restrictions on cross-border transfers but doesn’t require database registration, the establishment of a DPO or data security breach notification.
choice to provide notice in the event of a breach of secu-
rity resulting in unauthorized access to; alteration, dis-
closure of personal information that creates a risk of
harm' to affected individuals. Organizations must also
notify government institutions and other organizations
in prescribed circumstances, including where the orga-
nization believes that the government institution or
other organization may be able to reduce or mitigate the
harm to affected individuals. Until these amend-
ments come into force, there is currently no legal obli-
gation to give notice in the event of a data security
breach; however, the DPA has issued voluntary breach
notification guidelines.

The Guidelines recommend that notice be given when
there is unauthorized access to or collection, use or dis-
closure of personal information in a manner that sub-
stantially undermines personal privacy and the organiza-
tion in question is responsible for the entity.

In Brief

In June 2015, Parliament passed amendments to the Ca-
nadian Law requiring mandatory breach notification,
which will come into force as a data security breach or
in other circumstances, including where the organiza-
tion believes that the government institution or
other organization may be able to reduce or mitigate the
harm to affected individuals. Until these amend-
ments come into force, there is currently no legal obli-
gation to give notice in the event of a data security
breach; however, the DPA has issued voluntary breach
notification guidelines.

The Guidelines recommend that notice be given when
there is unauthorized access to or collection, use or dis-
closure of personal information in a manner that sub-
stantially undermines personal privacy and the organiza-
tion in question is responsible for the entity.

In Brief

In June 2015, Parliament passed amendments to the Ca-
nadian Law requiring mandatory breach notification,
which will come into force as a data security breach or
in other circumstances, including where the organiza-
tion believes that the government institution or
other organization may be able to reduce or mitigate the
harm to affected individuals. Until these amend-
ments come into force, there is currently no legal obli-
gation to give notice in the event of a data security
breach; however, the DPA has issued voluntary breach
notification guidelines.

The Guidelines recommend that notice be given when
there is unauthorized access to or collection, use or dis-
closure of personal information in a manner that sub-
stantially undermines personal privacy and the organiza-
tion in question is responsible for the entity.

In Brief

In June 2015, Parliament passed amendments to the Ca-
nadian Law requiring mandatory breach notification,
which will come into force as a data security breach or
in other circumstances, including where the organiza-
tion believes that the government institution or
other organization may be able to reduce or mitigate the
harm to affected individuals. Until these amend-
ments come into force, there is currently no legal obli-
gation to give notice in the event of a data security
breach; however, the DPA has issued voluntary breach
notification guidelines.

The Guidelines recommend that notice be given when
there is unauthorized access to or collection, use or dis-
closure of personal information in a manner that sub-
stantially undermines personal privacy and the organiza-
tion in question is responsible for the entity.

In Brief

In June 2015, Parliament passed amendments to the Ca-
nadian Law requiring mandatory breach notification,
which will come into force as a data security breach or
in other circumstances, including where the organiza-
tion believes that the government institution or
other organization may be able to reduce or mitigate the
harm to affected individuals. Until these amend-
ments come into force, there is currently no legal obli-
gation to give notice in the event of a data security
breach; however, the DPA has issued voluntary breach
notification guidelines.

The Guidelines recommend that notice be given when
there is unauthorized access to or collection, use or dis-
closure of personal information in a manner that sub-
stantially undermines personal privacy and the organiza-
tion in question is responsible for the entity.

In Brief

In June 2015, Parliament passed amendments to the Ca-
nadian Law requiring mandatory breach notification,
which will come into force as a data security breach or
in other circumstances, including where the organiza-
tion believes that the government institution or
other organization may be able to reduce or mitigate the
harm to affected individuals. Until these amend-
ments come into force, there is currently no legal obli-
gation to give notice in the event of a data security
breach; however, the DPA has issued voluntary breach
notification guidelines.

The Guidelines recommend that notice be given when
there is unauthorized access to or collection, use or dis-
closure of personal information in a manner that sub-
stantially undermines personal privacy and the organiza-
tion in question is responsible for the entity.

In Brief

In June 2015, Parliament passed amendments to the Ca-
nadian Law requiring mandatory breach notification,
which will come into force as a data security breach or
in other circumstances, including where the organiza-
tion believes that the government institution or
other organization may be able to reduce or mitigate the
harm to affected individuals. Until these amend-
ments come into force, there is currently no legal obli-
gation to give notice in the event of a data security
breach; however, the DPA has issued voluntary breach
notification guidelines.

The Guidelines recommend that notice be given when
there is unauthorized access to or collection, use or dis-
closure of personal information in a manner that sub-
stantially undermines personal privacy and the organiza-
tion in question is responsible for the entity.

In Brief

In June 2015, Parliament passed amendments to the Ca-
nadian Law requiring mandatory breach notification,
which will come into force as a data security breach or
in other circumstances, including where the organiza-
tion believes that the government institution or
other organization may be able to reduce or mitigate the
harm to affected individuals. Until these amend-
ments come into force, there is currently no legal obli-
gation to give notice in the event of a data security
breach; however, the DPA has issued voluntary breach
notification guidelines.

The Guidelines recommend that notice be given when
there is unauthorized access to or collection, use or dis-
closure of personal information in a manner that sub-
stantially undermines personal privacy and the organiza-
tion in question is responsible for the entity.

In Brief

In June 2015, Parliament passed amendments to the Ca-
nadian Law requiring mandatory breach notification,
which will come into force as a data security breach or
in other circumstances, including where the organiza-
tion believes that the government institution or
other organization may be able to reduce or mitigate the
harm to affected individuals. Until these amend-
ments come into force, there is currently no legal obli-
gation to give notice in the event of a data security
breach; however, the DPA has issued voluntary breach
notification guidelines.

The Guidelines recommend that notice be given when
there is unauthorized access to or collection, use or dis-
closure of personal information in a manner that sub-
stantially undermines personal privacy and the organiza-
tion in question is responsible for the entity.

In Brief

In June 2015, Parliament passed amendments to the Ca-
nadian Law requiring mandatory breach notification,
which will come into force as a data security breach or
in other circumstances, including where the organiza-
tion believes that the government institution or
other organization may be able to reduce or mitigate the
harm to affected individuals. Until these amend-
ments come into force, there is currently no legal obli-
gation to give notice in the event of a data security
breach; however, the DPA has issued voluntary breach
notification guidelines.

The Guidelines recommend that notice be given when
there is unauthorized access to or collection, use or dis-
closure of personal information in a manner that sub-
stantially undermines personal privacy and the organiza-
tion in question is responsible for the entity.

In Brief

In June 2015, Parliament passed amendments to the Ca-
nadian Law requiring mandatory breach notification,
which will come into force as a data security breach or
in other circumstances, including where the organiza-
tion believes that the government institution or
other organization may be able to reduce or mitigate the
harm to affected individuals. Until these amend-
ments come into force, there is currently no legal obli-
gation to give notice in the event of a data security
breach; however, the DPA has issued voluntary breach
notification guidelines.

The Guidelines recommend that notice be given when
there is unauthorized access to or collection, use or dis-
closure of personal information in a manner that sub-
stantially undermines personal privacy and the organiza-
tion in question is responsible for the entity.

In Brief

In June 2015, Parliament passed amendments to the Ca-
nadian Law requiring mandatory breach notification,
transfers to countries that don't provide adequate protection. In addition, some additional data security measures are required.

Special Characteristics
- **Data Protection Authority**
  - The Personal Data Protection Division, the organization within the Superintendence of Industry and Commerce responsible for performing the functions of the DPA, is authorized to carry out investigations on the basis of complaints or in its own initiative.

**Cross-Border Transfers**
- The transfer of personal information to countries outside Colombia that do not provide an adequate level of data protection is prohibited, unless the individual has provided his/her express consent to the transfer, the transfer is necessary to execute a contract between the individual and the organization or another exception applies. The DPA may approve transfers to non-adequate countries that don't fall under one of the above-listed exceptions by issuing a conformity declaration (declaración de conformidad). The additional requirements and obligations that must be satisfied before the DPA may issue such declarations are expected to be addressed in the forthcoming implementing regulations.

**Data Security**
- The DPA is required to issue instructions related to the security measures for processing personal information. If an organization breaches its duties and obligations under the law and the DPA has to decide whether or not to impose penalties, it will take into account the extent to which the organization has in place the proper security policies and measures for the proper handling of the personal information.

**Data Security Breach Notification**
- Both the organization and the service providers must inform the DPA about any violations of security codes and any risks in the administration of information of individuals. In order to be considered valid, the notification must be registered with the DPA.

**Registration**
- Organizations and service providers that carry out processing of personal information in Colombia are required to register with the DPA. The National Register was officially launched in November 2015.

---

**COSTA RICA**

Law No. 8968 on the Protection of the Person Concerning the Treatment of Personal Data (Costa Rican Law) came into force Sept. 5, 2011 (11 WDPR 17, 10/28/11). It applies to automatic and manual processing of personal information of natural persons in both public and private entities. Companies had until March 5, 2013 to bring their practices into compliance with the Costa Rican Law.

In Brief
- The Costa Rican Law requires data breach notification and registration. It also imposes special data security and "Su-
  per User" obligations but doesn't require the appointment of a DPO or restrict cross-border transfers. However, there are general rules that apply to all transfers.

Special Characteristics
- **Data Protection Authority**
  - Prodhab, established in March 2012, is responsible for creating a database registry, ensuring compliance with the Costa Rican Law and issuing implementing regulations.

**Cross-Border Transfers**
- There are no limitations on cross-border transfers; however, the general rules for any transfer of databases and/or personal information apply. In particular, express written consent (or a contract) is required to share or transfer personal information. The Costa Rican Law does not include any other legal bases for transferring data, and it applies to transfers within and outside Costa Rica.

**Data Security**
- In addition to the basic security obligations, the Costa Rican Law requires organizations to prepare a "Performance Protocol" that will regulate all the measures and rules to be followed in the collection, management, and handling of the personal information. In order to be considered valid, the Performance Protocol (and any subsequent amendments) must be registered with the DPA.

**Data Security Breach Notification**
- Organizations and service providers that carry out processing of personal information in Costa Rica are required to inform the DPA about any violations of security codes and any risks in the administration of information of individuals. In order to be considered valid, the notification must be registered with the DPA.

**Registration**
- Every database that is established for distribution, promotion or commercialization purposes must be regis-
tered with the DPA. According to a FAQ posted on the DPA website, human resources databases that are used for the exclusive use of the company do not need to be registered.

'Super User'
The Costa Rican Law has a very unusual requirement not found in any other privacy law worldwide. Organizations that registered databases with the DPA must provide the regulator with an access profile so that the DPA may access and consult the database, at any time and without restrictions. The FAQ issued by the DPA states that it will only access databases in response to a complaint or when there is evidence of possible law violations. It further states that the ‘Super User’ provision should not be interpreted as providing the DPA with absolute power to access all information contained in these databases. In particular, the DPA does not have the ability to access databases containing information regarding transactions, suppliers and corporate financial statements.

CURACAO
The Personal Data Protection Act (Curacao Law), which took effect Oct. 1, 2013, regulates the processing of personal information of natural persons by both the public and private sectors. The Curacao Law is modeled on the Dutch Data Protection Law.

In Brief
The Curacao Law restricts the cross-border transfer of personal information to countries that don't provide adequate protection. However, there are no DPO, data security breach notification and registration requirements. There is also no required timeframe specified for responding to access or correction requests.

Special Characteristics
Cross-Border Transfer
Personal information may only be transferred internationally in certain circumstances such as:

- the individual consent to authorize the transfer of information or when the laws so allow;
- the transfer is necessary for the execution of a contract between the individual and the organization, or for the execution of pre-contractual measures;
- the transfer concerns bank or security transfers with regard to the respective transactions and in accordance with the applicable legislation.

DOMINICAN REPUBLIC
The Organic Law 172-13 on the Protection of Personal Data (Dominican Law), which took effect Dec. 13, 2013, regulates credit information companies, the provision of credit reference services and the supply of information on the market to ensure respect for privacy and the rights of the information owners.

In Brief
In contrast to the cross-border rules found in other countries in the region, the Dominican Law imposes a common set of legal bases for all international transfers, regardless of their destination. Registration/supervision requirements apply only to public or private data banks that are regulated by financial regulations. Both data banks are subject to the inspection and supervision of the Superintendence of Banks.

Special Characteristics
Cross-Border Transfer
Personal information may only be transferred internationally in certain circumstances such as:

- for individual credit reference agencies in order to enforce or administer a contract to which the individual is a party or in order to enter into a contract with the individual;
- the transfer is necessary for the execution of a contract between the individual and the organization, or for the execution of pre-contractual measures;
- the transfer concerns credit information companies, the provision of credit reference services and the supply of information on the market to ensure respect for privacy and the rights of the information owners.
the transfer has been agreed or considered in the framework of international treaties or conventions, or in hierarchical relations of which the Dominican Republic is a party to.

The transfer of legally required information is to safeguard public interest or to exercise or defend a right in a judicial process, or is required for access to a public administration as well as for activities of public and private entities (Decree 106, 1995).

MEXICO

The Federal Law on Protection of Personal Data Held by Private Entities, enacted in 2012, regulates the processing of personal information of natural persons by private sector organizations and provides a framework for access and correction requirements and the appointment of a Data Protection Officer or Office. The DPA may take into account the organization’s compliance with DPA recommendations to determine the attenuation of the corresponding sanction.

In Brief

The data protection rules in the Mexican Law have a number of important differences from their United States analogs. For example, the notice and data security obligations are largely subject to the same requirements. The DPA has defined what constitutes personal information, the use of which requires the individual to be informed by the organization so the individual can take appropriate action to protect his or her rights. The Mexican Law does not require notice to the data protection authorities or regulator.

Special Characteristics

Data Protection Officer or Office

The DPA recommends that organizations appoint aData Protection Officer or Office for the creation of a bureaucratic air for Personal Data Protection within the Ministry of National Affairs.

Data Security Breach Notification

Organizations must inform the DPA of any security breaches involving personal information when there is a risk of material harm to the individual. The DPA will determine the attenuation of the corresponding sanction.

NIGERIA

The Nigerian Law on Personal Data Protection (Act No. 8.4) and the Regulations of the Law on Personal Data Protection (Order No. 36/2011) (Nigerian Law) established the Data Protection Office or Office to exercise their rights under the Nigerian Law.

Data Security

The Nigerian Law requires any entity that collects personal information to appoint a DPO or office to process requests (such as access and correction requests) and to exercise their rights under the Nigerian Law.
The Peruvian Law requires registration and restricts cross-border transfers. The DPA has established data security breach notification requirements. There is no obligation to appoint a DPO.

Data Protection Authority

The Peruvian Law established the National Authority for Protection of Personal Data to oversee compliance with the Law and investigate complaints lodged by individuals. The DPA is responsible for the regulation, supervision, and imposing administrative sanctions in cases of violation. The Peruvian Law requires registration and restricts cross-border transfers. The DPA has also established data security breach notification requirements. There is no obligation to appoint a DPO.

Cross-Border Transfers

Cross-border transfers of personal information are allowed if the recipient is a public and private sector organization, including where the transfer is necessary to carry out epidemiological investigations. The Peruvian Law establishes the National Authority for Protection of Personal Data to oversee compliance with the Law and investigate complaints lodged by individuals. The DPA is responsible for the regulation, supervision, and imposing administrative sanctions in cases of violation. The Peruvian Law requires registration and restricts cross-border transfers. The DPA has also established data security breach notification requirements. There is no obligation to appoint a DPO.

Data Protection Authority

The Peruvian Law established the National Authority for Protection of Personal Data to oversee compliance with the Law and investigate complaints lodged by individuals. The DPA is responsible for the regulation, supervision, and imposing administrative sanctions in cases of violation. The Peruvian Law requires registration and restricts cross-border transfers. The DPA has also established data security breach notification requirements. There is no obligation to appoint a DPO.

Cross-Border Transfers

Cross-border transfers of personal information are allowed if the recipient is a public and private sector organization, including where the transfer is necessary to carry out epidemiological investigations. The Peruvian Law establishes the National Authority for Protection of Personal Data to oversee compliance with the Law and investigate complaints lodged by individuals. The DPA is responsible for the regulation, supervision, and imposing administrative sanctions in cases of violation. The Peruvian Law requires registration and restricts cross-border transfers. The DPA has also established data security breach notification requirements. There is no obligation to appoint a DPO.

Data Protection Authority

The Peruvian Law established the National Authority for Protection of Personal Data to oversee compliance with the Law and investigate complaints lodged by individuals. The DPA is responsible for the regulation, supervision, and imposing administrative sanctions in cases of violation. The Peruvian Law requires registration and restricts cross-border transfers. The DPA has also established data security breach notification requirements. There is no obligation to appoint a DPO.

Cross-Border Transfers

Cross-border transfers of personal information are allowed if the recipient is a public and private sector organization, including where the transfer is necessary to carry out epidemiological investigations. The Peruvian Law establishes the National Authority for Protection of Personal Data to oversee compliance with the Law and investigate complaints lodged by individuals. The DPA is responsible for the regulation, supervision, and imposing administrative sanctions in cases of violation. The Peruvian Law requires registration and restricts cross-border transfers. The DPA has also established data security breach notification requirements. There is no obligation to appoint a DPO.

Data Protection Authority

The Peruvian Law established the National Authority for Protection of Personal Data to oversee compliance with the Law and investigate complaints lodged by individuals. The DPA is responsible for the regulation, supervision, and imposing administrative sanctions in cases of violation. The Peruvian Law requires registration and restricts cross-border transfers. The DPA has also established data security breach notification requirements. There is no obligation to appoint a DPO.
Registration

All organizations must register with the DPA. In addition, organizations that voluntarily adopt codes of conduct to govern their transfers to affiliated entities must register them with the DPA.

URUGUAY

Law No. 18.331 on the Protection of Personal Data and Habeas Data Action (Uruguayan Law), enacted in 2008 and amended in 2010, regulates the processing of personal information of natural and legal persons by both the public and private sectors. Uruguay was the second country in South America to be recognized by the EU as providing an adequate level of protection for personal information transferred from the EU/EEA (12 WDPR 16, 9/21/12).

In Brief

The Uruguayan Law requires data security breach notification and registration and restricts cross-border transfers to countries that do not provide adequate protection. There is no requirement to appoint a DPO; however, the person responsible for the database is liable for violations of the provisions of the law, and his or her name will be identified in the registration.

Special Characteristics

Data Protection Authority

The Regulatory and Control Unit for the Protection of Personal Data was created as an entity decentralized from the Agency for the Development of Government of Electronic Management and Information Society and Knowledge (AGESIC).

Cross-Border Transfers

The transfer of personal information of any kind to countries or international organizations that fail to provide adequate levels of protection according to the standards of regional or international law in this area is prohibited except where the following cases apply:

- international judicial cooperation, according to the relevant international instrument, whether treaty or convention, subject to the circumstances of each case;
- exchange of medical data, when necessary for the treatment of the sick person and for reasons of public health or hygiene;
- bank or stock exchange transfers, in regard to the corresponding transactions and pursuant to the applicable legislation;
- agreements within the framework of international treaties to which the Republic of Uruguay is a party;
- international cooperation between intelligence agencies fighting against organized crime, terrorism and drug trafficking.

It also is possible to make international transfers of data in the following cases:

- the interested party has given his or her consent to the proposed transfer;
- the transfer is necessary for the execution of a contract between the interested party and the person responsible for the processing or to implement pre-contractual measures taken at the interested party’s request;
- the transfer is necessary to execute an agreement on behalf of the interested party or the person responsible for the processing and a third party;
- the transfer is necessary to safeguard an important public interest, or for the recognition, exercise or defense of a right in a legal procedure;
- the transfer is necessary to safeguard the vital interests of the interested party; or
- the transfer is effected from a record which, by virtue of legal or regulatory provisions, is designed to provide information to the public and is open to consultation by the general public or any person who can prove a legitimate interest, provided that the conditions established by law for consultation are met in each particular case.

Regardless of the cases listed above, the DPA may authorize a transfer or a series of transfers of personal information to a third country that does not guarantee an adequate level of protection when the person responsible for the processing offers sufficient guarantees regarding the protection of privacy, fundamental rights and freedoms of individuals as well as to the exercise of the corresponding rights.

Such guarantees may arise from appropriate contractual clauses.

Data Security Breach Notification

When the data controllers or data processors realize that there has been a data security breach that could affect the individual’s rights in a significant way, the data controller or the data processor must inform the individual.

Registration

All organizations that create, modify or eliminate databases of personal information must register their databases.