Chapter 15

Privacy protection

This chapter focuses on policy measures to protect privacy. It introduces the main elements of a government policy framework to protect privacy and provides an overview of the situation in the LAC region. Finally, it provides a set of good practices, with a focus on the need to promote privacy risk management as a useful and relevant methodology for all data controllers to protect privacy.
The increased collection and processing of personal data for economic and social activities that rely on the digital environment raises a number of privacy challenges. These must be addressed both to protect fundamental values and individual liberties, and to ensure a digital environment that inspires confidence and in which individuals can fully participate. Privacy protection frameworks, also known as “data protection” frameworks, aim to create the conditions for public and private organisations to process personal data to pursue economic and social objectives while protecting privacy. In general, they set the requirements that organisations must respect when they collect, process and share personal data, as well as the rights granted to individuals. Although privacy protection frameworks are generally developed at the national level, flows of personal data often cross borders, raising the issue of the interoperability of these frameworks. In addressing this, policy makers face a double challenge: i) developing a framework that protects privacy while promoting economic development; and ii) ensuring a sufficient level of international interoperability to prevent the privacy protection framework from hindering blocking or inhibiting international trade.

The OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (hereinafter OECD Privacy Guidelines) aim to assist policy makers in the development of privacy frameworks (OECD, 2013). They were initially adopted in 1980 and revised in 2013. They define key concepts used in this area (“personal data”, “data controller” and so on) and include principles that can be used as a basis for privacy protection frameworks worldwide. The OECD Privacy Guidelines are high-level policy recommendations that can be used as a basis to develop a privacy protection framework with the flexibility to accommodate regional and local variations. Meanwhile, they should facilitate international interoperability for transborder flows of personal data. Most regional conventions, recommendations and standards for privacy and data protection are in line with the Privacy Guidelines, including the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter Convention 108) (CoE, 1981), the United Nations Guidelines concerning Computerized Personal Data Files (UN, 1990), the Asia-Pacific Economic Co-operation (APEC) Privacy Framework (APEC, 2005), the International Standards on Privacy and Data Protection (hereinafter the Madrid Resolution) (AEPD and PFPDT, 2009) and more recently, the Organization of American States’ (OAS) Model Law on Data Protection (OAS, 2014).

It is important to underline that privacy protection frameworks generally intersect with other frameworks, for example those governing digital security risk management (OECD, 2015), broadband policy and consumer protection, as well as with policies related to specific economic sectors such as health or finance.

This section presents a set of policy objectives, tools and measures for assessment in meeting key objectives to advance policies on privacy, data protection and e-identity. It provides an overview of the situation in the region based on national and regional indicators, points to good practices in the Latin America and Caribbean (LAC) region and establishes recommendations based on the work of international and regional organisations like the OECD and OAS.
Key policy objectives in the LAC region

Privacy protection is regulated in relevant instruments on international public law, such as the Universal Declaration of Human Rights (UN, 1948), the International Covenant on Civil and Political Rights (UN, 1966a), the International Covenant on Economic, Social and Cultural Rights (UN, 1966b) and the Inter-American Convention on Human Rights (OAS, 1969). It is therefore essential to ensure the continuity of privacy protection from the offline to the digital environment. However, the main policy objective is to develop and implement a policy framework that protects privacy while i) encouraging the use of the digital environment for economic and social prosperity; and ii) enabling transborder flows of personal data through appropriate international policy and legal interoperability. This general policy goal can be met through policy tools, such as:

Developing a national privacy strategy

A national privacy strategy that reflects a co-ordinated approach across governmental bodies is one of the key measures of national implementation included in the OECD Privacy Guidelines. Elements of the national strategy can include:

- the adoption of laws protecting privacy
- the establishment of privacy enforcement authorities with the governance, resources and technical expertise to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis
- the encouragement and support of self-regulation
- the provision for adequate sanctions and remedies in case of failure to comply with laws protecting privacy
- the adoption of complementary measures, including education and awareness campaigns, skills development and the promotion of technical measures, that help to protect privacy.

Implementing accountability

Accountability is one of the key principles of the OECD Privacy Guidelines. Data controllers should be accountable for complying with measures that enshrine the other OECD privacy principles. A privacy protection framework can encourage data controllers to implement accountability by:

- setting up a privacy management programme
- being prepared to demonstrate the propriety of its privacy management programme, in particular at the request of a competent privacy enforcement authority or other entity responsible for promoting adherence to a code of conduct or similar arrangement that gives binding effect to the Guidelines
- providing notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects.

Free flow and legitimate restrictions

Recognising that a data controller remains accountable for personal data under its control without regard to the location of the data, the OECD Privacy Guidelines call on countries to refrain from restricting transborder flows of personal data (TBDF) between
themselves and another country and for any restrictions to TBDF to be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.\textsuperscript{10}

**International co-operation and interoperability**

LAC countries should co-operate in the enforcement of privacy laws and facilitate international interoperability of privacy frameworks. This implies, for example:

- taking appropriate measures to facilitate cross-border privacy law enforcement co-operation, in particular by enhancing information sharing among privacy enforcement authorities
- encouraging and supporting the development of international arrangements that promote interoperability among privacy frameworks that give practical effect to the OECD Privacy Guidelines
- encouraging the development of internationally comparable metrics to inform the policy making process related to privacy and transborder flows of personal data
- making public the details of their observance of the international or national privacy guidelines.

**Tools for measurement and analysis for the LAC region**

There is no general agreement on indicators to measure the various aspects of privacy protection policy frameworks. However, in the context of their reporting and transparency obligation, privacy enforcement authorities generally publish an annual report reflecting their activities. This includes statistics on, for example:

- number of complaints received
- number of requests for information from individuals and data controllers
- number of fines, etc.

Unfortunately, the methodologies to collect and aggregate data are generally not comparable, and there is no systematic comparative analysis of these statistics, whether at the regional or international level.

**Overview of the situation in the LAC region**

**National privacy strategies**

None of the countries in the LAC region have a comprehensive national privacy strategy or programme. This is not surprising considering that the concept of national privacy strategy is relatively new. However, the proportion of LAC countries with privacy and data protection legal frameworks in place is relatively high (around 40%), and the number is growing.

Nine countries (Colombia, Costa Rica, Chile, the Dominican Republic, Ecuador, Mexico, Nicaragua, Peru and Uruguay) have privacy and data protection laws, including supervisory or regulatory authorities (Box 15.1). Brazil, Chile, Jamaica and Paraguay are in the process of consultation and drafting new laws in this area.

The great majority of countries in the LAC region, for example Brazil, Panama and El Salvador, have sectoral laws with scattered provisions on privacy and data protection, but no independent laws and regulations so far on data protection and national data protection authorities (OAS, 2015).
Box 15.1. **Selected national laws and regulations on privacy and data protection (2010-15)**

**Colombia**
- Statutory Law No. 1581 containing General Provisions for the Protection of Personal Data (17 October 2012)
- Decree No. 1377 that Partially Regulates Statutory Law No. 1581 of 2012 (27 June 2013)
- Decree No. 866 that Regulates the National Registry of Databases pursuant to Article 25 of Statutory Law No. 1581 (13 May 2014).

**Costa Rica**
- Law No. 8968 of Protection of the Individual for the Processing of his Personal Data (5 September 2011)
- Regulation of Law No. 8968 contained in Executive Decree No. 37554-JP (30 October 2012).

**Dominican Republic**

**Mexico**
- Federal Law on Data Protection in the Possession of Private Parties (5 July 2010)
- Regulation of the Federal Law on Data Protection in the Possession of Private Parties (19 December 2011)
- Self-Regulation Standards on Protection of Personal Data (29 May 2014).

**Nicaragua**
- Law No. 787 on Protection of Personal Data (29 March 2012).

**Peru**
- Regulation of Law No. 29733 of Protection of Personal Data (22 March 2013)
- Law No. 29733 of Protection of Personal Data (3 July 2011).

Law enforcement continues to be a challenge in the LAC region. The proportion of countries with an independent national Data Protection Authority (hereinafter DPA) is very low. Only two countries (Mexico and Uruguay) have a fully independent and autonomous DPA. In other countries, the DPA is part of a ministry, as in Colombia (Ministry of Economy), Costa Rica and Peru (Ministry of Justice) and Ecuador (Ministry of Telecommunications and Information Society).

Policy makers in the LAC region tend to view privacy and data protection as a legislative and regulatory issue, rather than from the economic and social public policy perspective.

**Implementing accountability**

The concept of accountability has not yet gained wide acceptance in the LAC region. Only Mexico\(^{11}\) incorporates this concept in its national data protection legislation and regulation. Colombia recently published a guide for the implementation of accountability in organisations as part of the implementation of Articles 26 and 27 of Decree No. 1377 of 27 June 2013 (SIC, 2014). However, the extent of the use of this principle by data controllers is not entirely clear. The implementation of a privacy management programme is not compulsory under most data protection laws of LAC countries.
Free flow of data and legitimate restrictions

There are remarkable differences of approach to the regulation of transborder data flows and restrictions on the transfer of personal data from LAC countries to third countries. The proportion of countries with restrictions and regulations on the free flow of information is quite high. Six countries (Argentina, Colombia, Costa Rica, Mexico, Peru and Uruguay) have provisions that stipulate special conditions for national and international transfers of personal data, as well as the use of mechanisms to export information to third countries, which includes model contractual agreements and clauses and binding corporate rules (Velasco, 2015).

International co-operation and interoperability

The proportion of countries with international co-operation agreements and other mechanisms for the exchange of information for the enforcement of cross-border privacy is very low. Only three LAC countries (Argentina, Colombia and Mexico) are part of the OECD’s Global Privacy Enforcement Network (GPEN).12

The concept of privacy interoperability has not yet gained wide acceptance in LAC countries. The proportion of LAC countries promoting interoperability with other privacy frameworks is very low. Only Mexico participates in the APEC’s Cross-Border Privacy Rules (CBPR) System (Box 15.2).13 This country is seeking the interoperability of its national framework on data protection – in particular the implementation of self-regulation schemes through certification agents – with APEC economies. Other LAC countries, such as Chile and Peru, are also members of the APEC.

Box 15.2. Countries on interoperability with other data protection frameworks

Mexico

Mexico, through the Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), participates in APEC’s Cross-Border Privacy Enforcement Arrangement (CPEA). This is a vehicle for regional co-operation in enforcing privacy laws among APEC member economies. Mexico is the only LAC country promoting interoperability with other data protection frameworks. Mexico’s Ministry of Economy has participated in APEC’s Cross-Border Privacy Rules (CBPR) System since February 2013.


Notification of data breaches and enforcement of data protection laws

Data security breaches are on the rise in LAC countries. Only three countries (Colombia, Costa Rica and Mexico) have established in their data protection legal framework obligations to notify affected data subjects and imprisonment sanctions for data controllers in case of a data breach (Box 15.3).
Box 15.3. **Selected laws and regulation with data breach notification obligations**

**Colombia**

Article 17(n) of Statutory Law No. 1581 establishes the obligation for data controllers to inform data protection authorities when security breaches occur and present risks in the administration of information of data subjects. Article 18(k) establishes an obligation to inform the Superintendencia de Industria y Comercio (DPA) when security breaches occur and to present risks in the administration of information of data subjects. The law provides fines for the equivalent of 2,000 days of minimum wage and the suspension of activities for six months.


**Costa Rica**

Articles 38 and 39 of Regulation of Law No. 8968 of Protection of the Individual for the Processing of his Personal Data establish an obligation for data controllers to inform data subjects on any irregularity in the processing and storage of their personal data as a result of a security vulnerability within five working days from the day the vulnerability occurred, to initiate a comprehensive review to determine the magnitude of the breach and the corrective and preventive measures to be taken and to inform both data subjects and the DPA (PRODHAB).


**Mexico**

Article 20 of the Federal Law on Data Protection in Possession of Private Entities (FLDPPPP) establishes obligations for data controllers to immediately inform data subjects in case of a data breach. Articles 67 and 69 of the FLDPPPP set forth imprisonment sanctions from three months to three years. The punishment may be doubled when sensitive information is involved. The former IFAI (now INAI) used the data breach notification provision of the FLDPPPP to request from Sony Mexico a report of the affected users located in national territory when the data breach scandal of Sony’s Play Station Network and Qriocity occurred between 17 and 19 April 2011.

INAI enforced the data breach notification provisions of the FLDPPPP to request the national retailer Puerto de Liverpool S.A.B. information regarding the status of its databases containing personal information of employees and customers as a result of a data breach that occurred in December 2014.


Although enforcement of data protection laws still needs to be improved in LAC countries, some DPAs have started to levy fines and sanctions for noncompliance against data processors and data controllers (Box 15.4).

**Summary of the overall situation**

In recent years, many LAC countries have passed laws, regulations and policies to protect privacy and personal data as a fundamental human right, in line with various international and regional instruments on data protection. Brazil, Colombia, Costa Rica, the Dominican Republic, Ecuador, Mexico, Nicaragua, Peru and Uruguay are among the LAC countries with data protection legislation and regulation in force.
Box 15.4. Selected NDPAs levying sanctions for noncompliance with data protection laws

Mexico

Mexico’s DPA (INAI) is perhaps one of the leading enforcement authorities in the region. INAI reports a total of 21 sanction procedures for an estimate amount of USD 6.6 million (MXP 108.3 million) from January 2012 to 22 May 2015, divided into the following segments:

- insurance and financial services: USD 3.17 million (14 sanction procedures)
- massive media and information sector: USD 1.86 million (4 sanction procedures)
- education services sector: USD 612,394 (3 sanction procedures).


Peru

Despite the recent enactment of the Regulation of Law No. 29733 of Protection of Personal Data, the DPA in Peru reports five procedures resulting in economic sanctions and fines against data controllers.


Only one country (Mexico) has moved to a pro-active co-regulatory approach that includes the use and implementation of binding self-regulation on data protection. It has minimal regulatory restrictions on cross-border data flows, to facilitate trade and the exchange of data with third countries while encouraging technology innovation. However, the majority of countries of LAC still face numerous challenges, including:

- pro-active enforcement of data protection laws and regulations by the DPA
- encouragement of privacy management programmes that include obligations to respond, notify and provide redress to data subjects in case of a security breach affecting personal information
- harmonised cross-border privacy co-operation with other DPAs and law enforcement authorities, and encouragement of interoperability with other regional and national frameworks on privacy and data protection (e.g. APEC’s Privacy Framework).

The majority of LAC countries have not developed national privacy strategies that take into consideration the recommendations in the OECD Privacy Guidelines. In addition, DPAs in LAC countries have not been conducting ongoing national campaigns for the protection of personal data that help to comply with the laws and regulations on privacy and data protection and to inform users about the mechanisms available to help them exercise their data protection rights.

Implementation of cross-border co-operation agreements to enforce privacy laws in LAC countries is limited. Only Argentina, Colombia and Mexico are members of the GPEN through their respective DPAs. National budget constraints are likely to be among the reasons for this, given that few countries have allocated annual budgets in this area.

In the field of cross-border data transfers, the legal frameworks of Peru and Colombia establish conditions to conduct international data transfers to third countries based on the adequacy level of protection contained in the European Union Data Protection Directive of 1995 and the draft European Union General Data Protection Regulation. Paradoxically, neither Colombia nor Peru has yet met the adequacy level of protection standard of
the European Commission. Only the data protection laws and regulations of Argentina\(^{17}\) and Uruguay\(^{18}\) have met the European Union adequacy decision standard. However, after the decision handed down by the Court of Justice of European Union (CJEU) in October 2015 (CJEU, 2015), some uncertainty remains over the status of the adequacy decisions related to Argentina and Uruguay.

The data protection laws of Colombia, Peru and Mexico contain provisions for the use of standard contractual clauses, binding corporate rules and other legal instruments to conduct international transfers of data to third countries. However, such mechanisms have not yet been fully implemented at a practical level, and the DPAs of LAC countries have not yet made official statements on the validity of such instruments.

**Good practices for the LAC region.**

Good regulatory practice in the area of privacy protection includes the promotion of privacy risk management\(^9\) by the policy makers of LAC countries, as a useful methodology for data controllers to protect privacy.\(^{20}\) This is perhaps one of the greatest challenges in the region, since it is a novel concept and the consensus is that “work is needed to understand practical applications and implications” of privacy risk management.

National privacy strategies should incorporate each of the policies contained in Part Five of Principle 19 of the OECD Revised Privacy Guidelines (Box 15.5).

---

**Box 15.5. Policy recommendations for national Implementation of the OECD privacy framework**

- Develop national privacy strategies that reflect a co-ordinated approach across governmental bodies
- adopt laws protecting privacy
- establish and maintain privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis
- encourage and support self-regulation, whether in the form of codes of conduct or otherwise
- provide for reasonable means for individuals to exercise their rights
- provide for adequate sanctions and remedies in case of failures to comply with laws protecting privacy
- consider the adoption of complementary measures, including education and awareness raising, skills development, and the promotion of technical measures that help to protect privacy
- consider the role of actors other than data controllers, in a manner appropriate to their individual role
- ensure that there is no unfair discrimination against data subjects.


The broad implementation of the accountability principle is also relevant. The actions contained in Principle 15 of the OECD Revised Privacy Guidelines need to be implemented by both data controllers and data processors (Box 15.6).
Box 15.6. **OECD Principles for Implementing Accountability**

A data controller should:

- Have in place a privacy management programme that:
  - gives effect to these Guidelines for all personal data under its control
  - is tailored to the structure, scale, volume and sensitivity of its operations
  - provides for appropriate safeguards based on privacy risk assessment
  - is integrated into its governance structure and establishes internal oversight mechanisms
  - includes plans for responding to inquiries and incidents
  - is updated in light of ongoing monitoring and periodic assessment.

- Be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines.

- Provide notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects.


Policy makers should encourage balanced policies on TBD and legal instruments, such as for example model contractual clauses and agreements and binding corporate rules for the transfer and process of personal data across different regions.

To encourage policies on privacy, active participation in international and regional enforcement networks on cross-border privacy networks is also important. These would include the GPEN and APEC’s Cross-Border Privacy Enforcement Arrangement (CPE) and national data protection laws’ interoperability with other regional data protection frameworks to reinforce the protection of personal information of data subjects across borders.

**Conclusion**

This chapter focused on policy measures to develop and implement a policy framework that protects privacy while encouraging the use of the digital environment for economic and social prosperity and enabling transborder flows of personal data through appropriate international policy and legal interoperability. It introduced the main elements of a privacy policy framework: a national privacy strategy including relevant legislation and a privacy enforcement authority, measures to encourage self-regulation and the adoption of privacy management programmes to increase accountability by data controllers, as well as mechanisms to facilitate interoperability of privacy frameworks across borders.

In addition, after underlining the lack of indicators to measure the various aspects of privacy protection, this chapter provided an overview of the situation in the LAC region. While no LAC country has yet developed a national privacy strategy, a relatively new concept, several have associated legislation and a privacy enforcement authority and others are currently developing their framework. Only a few countries in the region are part of an international co-operation agreement, and the concept of accountability has not yet gained wide acceptance in the region.
Notes

1. This convention, like most European legal instruments on data protection, is currently going through a reform and modernisation process.

2. The Madrid Resolution was adopted on the 5 November 2009 at the annual meeting of the International Conference of Data Protection and Privacy Commissioners (ICDPPC), a global forum of field experts and the highest authorities and institutions guaranteeing data protection and privacy (AEPD and PFPDT, 2009).

3. See Article 12.

4. See Article 17.

5. See Article 5.

6. See Article 11.


8. According to the OECD Privacy Guidelines (OECD, 2013), a data controller is the “party who, according to national law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf”.


11. See Articles 6 and 14 of the Federal Law on Data Protection in Possession of Private Entities (FLDPPPP) and Articles 47 and 48 of the Regulation of the FLPPDP.

12. GREN was established as part of the implementation of the 2007 OECD Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (OECD, 2007). GREN’s website is available at www.privacyenforcement.net.


16. Ibid., note 45, p. 895.


19. In the opinion of the Centre for Information and Policy Leadership at Hunton & Williams, “the role of risk management is a valuable tool for calibrating the implementation of and compliance with privacy requirements, prioritizing action, raising and informing awareness about risks, identifying appropriate mitigation measures and, in the words of the Article 29 Working Party, providing a ‘scalable and proportionate approach to compliance’. See pp. 1-3 of Centre for Information Policy Leadership (2014).

20. Paragraph Six and Principle 15(a)(ii)(vi)(c) of the OECD Revised Privacy Guidelines takes into consideration the role of “risk assessment approach” in the development of policies and safeguards to protect privacy.

References


Centre for Information Policy Leadership (2014), The Role of Risk Management in Data Protection: A Privacy Risk Framework and Risk-based Approach to Privacy, Centre for Information Policy Leadership at Hunton & Williams.


Further reading

