The Information Accountability Foundation (“IAF”) is a non-profit research centre with the charitable purpose of research and education. It was founded in 2013 to further the work of the Global Accountability Dialogue that formulated the Essential Elements of Accountability. The IAF has a global mission and has been active in Latin America since its founding. Martin Abrams, IAF Executive Director, has advised numerous Latin American authorities for the past decade.

The IAF appreciates the opportunity to provide input to the review of the Argentina Personal Data Protection Law by the National Data Protection Authority. IAF’s comments will be confined to a narrow portion of the total legislation that links to the research work that it is conducting.

Comments are provided on the following three topics:

1. Including a preamble that establishes the legislative purposes for a data protection law that encompasses both individual autonomy and fair processing;
2. Creating a legal obligation for organizations that process data to be responsible and answerable through accountability obligations;
3. Establishing a legal basis to process personal information that goes beyond individual consent.

The IAF believes the combination of accountability and legal basis to process furthers national objectives to protect the full range of fundamental rights while encouraging economic growth in the current digital age. These suggested provisions would also mirror the requirements of the European Union’s new General Data Protection Regulation that goes into effect in May 2018. IAF’s comments also provide perspective on why changes in technology and business process make it useful to update the identified provisions.

**Protecting Individual Autonomy and Fair Processing**

All national privacy laws seek to protect individual autonomy and assure fairness when processing personal information. Individuals should be able to exercise control over their data whenever possible, and organisations have an obligation to process that data, whether there is consent or not, in a fashion that assures there is protection when data is collected, created,
stored, used and destroyed. Furthermore, data should be processed in a manner that enhance the benefits for all stakeholders – individuals, groups of individuals, society, and organisations – while mitigating risks to individuals and society. Fundamental rights go beyond a narrow definition of privacy. Healthcare, education, shared benefits from technology are all tied to fundamental rights. Individual control assures autonomy, while fair processing assures the full range of rights and interests. Historically, the implementation of privacy law often focused on the first part, autonomy. However, the growth of data and the accelerating complexity of processing requires a renewed focus on fair processing.

The European Union, with its 1995 Data Protection Directive and 2016 General Data Protection Regulation, has established a laboratory for this concept of autonomy and fair processing. The EU law establishes privacy as a right directed at individual autonomy and assurance of family life. However, data protection laws, such as the Directive, had a much broader remit. Data protection is designed to protect the full range of fundamental rights impacted by the processing of personal information, not just privacy. To accomplish this objective, the law focuses on six legal basis to process, one of which is consent. The national laws that implemented the Directive often placed an emphasis on one legal basis, consent, to permit processing. However, the new General Data Protection Regulation is one set of rules to be enforced by the various national authorities, not 28 different local systems. Therefore, the concept of six legal basis is given much greater prominence in the law to go into effect in 2018.

The EU GDPR also continues the concept of data transfers being limited to countries with adequate data protection laws. Argentina was found adequate by the EU Commission as it related to the 1995 Directive. As Argentina looks to update its data protection legal regime it may prove useful to think about the more prominent role played by legal basis to process, for assuring adequacy, under the law going into effect in May 2018.

Canada, another country that was designated as adequate by the EU Commission and also has a consent based law is, is looking at the role of consent in a highly observational world where privacy notices cannot always capture the nuance in data use. The Office of the Privacy Commissioner issued a consultation paper in the Spring on the challenges to consent that may be helpful in your review. That consultation paper is attached in the form of an unofficial Spanish translation by the IAF. A Spanish translation of IAF’s comments to the Office of the Privacy Commissioner is also provided.

**IAF Recommendations**

The following recommendations for legislative change are offered pursuant to the IAF’s educational mission, which includes the furtherance of accountability based governance. These recommendations do not necessarily reflect the views of the IAF’s charitable funders, board of trustees, or the broader IAF family. As stated earlier, the focus is on three topics.

**Law should have a clear statement of objectives**
If possible, the law should include a preamble that clearly states the objectives to be achieved through the legislation. The objectives would surely include individual autonomy to assure dignity as one of the justifications for the law, but the objectives should also include that human dignity runs to the full range of fundamental rights and interests. The free flow of information to assure data is used to improve the full range of human interests including improved healthcare, education, and economic opportunity is a dual objective of the law. The language might read something like:

*Personal data is the life blood of a free economy and society. The thoughtful processing of personal information enhances data driven innovation with the potential to improve education, healthcare, economic growth, and the shared benefits of new technology. However, personal data used without respect for the fundamental right to privacy to assure individual dignity creates risks to the development of personality, personal freedom and a democratic society. The purpose of this law is to facilitate the use of personal data to enhance human development while protecting people from inappropriate data uses.*

**Accountability as an Explicit Data Protection Pillar**

Accountability was first adopted as an OECD privacy principle in 1980. Accountability was first explicitly represented in national privacy law in Canada’s private sector law entitled the Personal Information Protection and Electronic Documents Act (“PIPEDA”) in 2000. Accountability has since been expressly adopted in legislation in Mexico and the new EU General Data Protection Regulation. Canada defined regulator expectation in a 2012 advisory paper issued jointly by the federal Office of the Privacy Commissioner and provincial regulators entitled “Getting Accountability Right Through a Comprehensive Privacy Management Program.” That guidance has since been modified for local use by privacy authorities in Hong Kong and Colombia. To align with global trends, we believe Argentina should consider making accountability an explicit requirement. Doing so would also facilitate the IAF’s permissions.

Statutory accountability language might read something such as the following:

1. **Accountability means assuring a controller uses data in a manner that a reasonable person would consider responsible and in alignment with the context set by the privacy notice published by the organization and the general nature of the business;**
2. **The organization should be able to demonstrate a privacy and fair processing program that is proportional to the nature of the organization and the risk it creates for individuals;**
   a. An organisation’s demonstration of accountability would reflect the following five essential elements:
      i. Policies that align with the obligations set forth in this law to process personal data in a fair manner;
ii. Mechanisms to put those policies into place, including assessments of risks to individuals and society;

iii. A means for monitoring those mechanisms;

iv. Openness about the organisation’s use of data to set the context for data’s further uses, and facilitate individual participation through access and correction of the data that pertains to a particular individual;

v. Documentation of the program, and standing ready to demonstrate the program to the National Data Protection Authority.

b. Organisations that collect information in Argentina for a business or professional purpose must file the name of an individual who will be answerable for the organisation to the National Data Protection Authority;

   i. The filing should include contact information for that individual, along with the address, phone number and an email address of the organisation;

   ii. The filing should describe the general nature of the processing that will take place;

   iii. The National Data Protection Authority may collect reasonable fees for administration of the act as it relates to the oversight of organisations that must file;

   iv. Data registration requirements are replaced by this filing requirement.

Permission to Process

As stated earlier, the IAF suggests that Argentina should not limit the permission to process persona information to individual consent and statutory exemptions, but rather adopt a system based on several legal basis to process. Statutory language might read something like the following.

(1) The processing of personal data is permitted if one or more of the following five conditions is met:

   a. The individual has provided clear consent;

   b. The data is needed to fulfill a contract or the individual’s request;

   c. In response to a legal requirement;

   d. In the individual’s or society’s clear interest when consent is not possible or practical;

   e. For research purposes where:

      i. Tangible risks to the individual are assessed and mitigated;

      ii. There is a clear separation between the data used for research and that same data being used to have an impact that may have a legal effect on the same individuals to which the research data pertained;

         1. Unless there is a clear tangible risk to the individual that might be mitigated by contacting the individual;
iii. The assessment and protections required by this section are demonstrable to the National Data Protection Authority on request.

f. In the legitimate interests of an organization or society where:
   i. The processing creates real benefits for the organization, individuals and/or society as a whole;
   ii. Where processing is in the context of the relationship of persons to the organization;
   iii. Risks to persons and society are listed and mitigated if possible;
   iv. Where the benefits of the processing are clearly greater than residual risks;
   v. An assessment of these factors is available for review by the National Data Protection Authority on request.

The IAF would be delighted to discuss these recommendations with the National Data Protection Authority team. Martin Abrams, IAF Executive Director may be reached at mabrams@informationaccountability.org and +1.972.955.5654.
Attachments (in Spanish)

“Consentimiento y Privacidad”
“Consent and Privacy: A discussion paper exploring potential enhancements to consent under the Personal Information and Electronic Documents Act”

Consulta de Contribución de la IAF: “Consentimiento y Privacidad”

“Guía para la implementación del principio de responsabilidad demostrada”