



March 8, 2017

Dear Sirs and Madams:

The Information Accountability Foundation ("IAF") is pleased to be asked for its views regarding the draft guidance for the transfer or transmission of data from Colombia to other geographic locations (Draft Guidance). The IAF is a non-profit foundation whose charitable purposes are research and education in information policy. These comments reflect the views of the IAF staff and do not necessarily reflect the views of the IAF board of directors or funders.

IAF commends the Superintendency of Industry and Commerce (SIC) for a very thoughtful approach to the adequacy provisions in the Draft Guidance that is designed to achieve not only the protection but also facilitate the transfer of personal data. The free flow of information pertaining to individuals is essential to the provision of the full range of fundamental rights and commerce. Furthermore, the protection of that data requires constant vigilance. These comments are intended to be helpful as SIC considers the best means for assuring protection along with the benefits of data flows.

#### Accountability

The OECD Privacy Guidelines were designed to encourage the free flow of personal information across borders with appropriate protections in place. The OECD guidelines include an accountability principle to place the responsibility for the governance and protection of personal data on individual organizations. The Canadian private sector privacy law, the Personal Information Protection and Electronic Documents Act, uses accountability to govern transfers, placing responsibility on controllers to make sure that protections stay with data, no matter who processes the data and where the data is processed. To make sure protections stay with the data, controllers must conduct due diligence, including having contracts with processors. Accompanying these comments is the guidance issued by the Office of the Privacy Commissioner of Canada on accountability as it relates to the movement of data.

Colombia's privacy law requires personal data on or about Colombians to be protected and used appropriately no matter where that data is processed. To accomplish that objective, Colombian law prohibits transfers to countries that lack adequate privacy protections. To add some flexibility without diluting the protections contained in the law, the implementing regulations differentiated between transfers and transmissions. This flexibility is one of the strengths of the implementing regulations.

After talking with various parties, the IAF staff is concerned that the Draft Guidance does not make it clear that Colombian law partners the concepts of adequacy with that of accountability. The confusion may originate from the fact that the Draft Guidance specifies that contracts are necessary with transmissions but does not mention that contracts also are necessary for transfers. This has led some parties to believe that transfers to countries deemed adequate do not require a controller to make sure other parties touching the data are doing so consistent with the obligations associated with the data. That is assuredly not the case. All organizations moving data are to be held to account. So, as it relates to contracts, there are no differences between transfers and transmissions. IAF staff believes making accountability clear in the final guidance would be an improvement.

One way that organizations demonstrate they are accountable are essentially internal codes that link with external criteria. Examples of such codes are European Binding Corporate Rules and APEC Cross Border Privacy Rules. SIC may want to consider recognizing those codes to encourage a higher level of transparency as it relates to the means to demonstrate that data is being protected.

#### White Lists and Criteria

The Draft Guidance includes the criteria necessary to determine whether a country has adequate privacy protections as well as a list of 38 countries that are deemed adequate. The Draft Guidance also puts the burden of determining whether a country is adequate on the organizations that wish to transfer data.

After reviewing the list of adequate countries, IAF staff are unable to ascertain how SIC applied the criteria to arrive at the list of countries. Many of the countries are part of the European Union, while other countries have been deemed adequate by the Commission of the European Union. However, there are some countries on the EU white list, such as Israel and the Isle of Man, that are not on the proposed Colombian white list. Furthermore, the purpose of the criteria is to require destinations to protect information in a manner expected by Colombian nationals.

IAF staff make the following observations related to the criteria, white lists, and means for companies to determine whether a country is adequate:

1. White lists tend to create a safe harbor. As a result, companies may feel compelled to use processors within the safe harbor even if they are not the processors with the best security processes in place. For example, a cloud provider within the safe harbor with dated security mechanisms is not a better choice than a cloud provider with very sound security mechanisms in a country where privacy is respected but not on the white list.
2. Criteria (f), the existence of public authorities, does not ask whether these authorities have the resources to fulfill their mission or even to pursue investigations on behalf of SIC. The importance of real protection is an emphasis of the Colombia Constitutional Court decision C-748 of 2011 that states: "... a protection procedure that involves mechanisms and authorities that effect the protection of information."
3. The white list does not explain how SIC evaluated the 38 countries on the list or why some countries with well-established privacy mechanisms were not included on the white list.
4. Many of the countries on the white list have laws that require adequacy but do not recognize Colombia as adequate.

Bottom-line, IAF staff is concerned that the presence of a white list will replace due diligence related to accountability. IAF staff understand that this is not SIC's objective, but it may be the result.

IAF staff make the following recommendations:

1. Build accountability into the guidance. Make clear that both transfers and transmissions require due diligence and contracts that make sure obligations that come with data are respected.
2. Consider how to make more use of accountability by recognizing the effectiveness of codes of conduct related to transfers.
3. In considering adequacy, SIC may want to place an emphasis on mechanisms and means for oversight and enforcement in the countries being reviewed.
4. Consider the impact white lists will have on the protected flow of personal information to and from Colombia.
5. Consider amending the evaluation criteria to make sure protections are not just contained in law but also are implemented in a manner that provides protection, as suggested by the Constitutional Court.

Thank you for the opportunity to comment, and IAF staff would be most willing to discuss further.

Sincerely,

A handwritten signature in dark ink, appearing to read 'M. Abrams', with a long horizontal flourish extending to the right.

Martin Abrams  
Executive Director