THE Information Accountability Foundation
COLLABORATIVE POLICY INNOVATION

July 31, 2017

Dear Sirs and Madams:

The Information Accountability Foundation (IAF) is aware that the Superintendence of Industry and Commerce (SIC) has issued new draft guidance on the transfer of data from Colombia to other geographic locations. The IAF commented extensively on the initial draft guidance, and I provide these comments in my personal capacity based on my long experience with SIC. They do not necessarily reflect the views of the IAF Board of Trustees or its funders.

I understand that the draft guidance includes the United States as one of the countries that has adequate privacy protections. I believe the United States has effective means for protecting individual privacy based on the Federal Trade Commission Act, sector specific protections, state laws, and other protections based on fair play. Based on IAF's earlier comments, SIC is also aware that I believe determining adequacy to be difficult at all times, and much more so because of the new technologies and business practices that have developed in this decade. So, I believe your findings regarding the United States a positive statement based on the concept of effective protection.

However, I am concerned there will be confusion regarding the compliance rigor related to transfers versus transmissions. Colombia is unique in having secondary regulations that include both data transmissions to processors and transfers to other controllers. Both means of moving data are covered explicitly by not only secondary regulations but also by the concepts central to accountability. This obligation is made clear by the reference in the draft guidance to Decree 1074 of 2015 that established the principle of accountability. An accountable organization is both responsible for being an effective data steward and answerable if data is used inappropriately or the security of the data is not protected.

My understanding is that the secondary regulations specifically require organizations transmitting data to enter into a contract requiring the data to be protected to the same level as if it were being processed by the controller. From an accountability perspective, this activity would be part of the due diligence required by a controller.

I believe, the draft guidance, by referencing Decree 1074, creates the same obligation for transfers. While not specifically stated in the draft guidance, from an accountability perspective, a transfer of data, even to a country with adequate privacy protection, would also require due diligence by the controller.

Such due diligence would require a Colombian controller to assure that the obligations associated with the data stay with the data. At the very least, this due diligence would typically require a contract. So, from an accountability perspective, there would be no less obligations on the party exporting the data in a transfer than in a transmission of data.

So, the question that arises is what assurances are needed when moving data beyond Colombia. I suggest that those assurances should be specific to the type of processing that will take place.

If data is transferred to a controller, agreements should assure that all the obligations that came with the data, including any specific requirements linked to Colombian law, are respected. The receiving controller must be obligated to respect those conditions.

Transmissions are more context specific. Some processors are an extension of the organization itself (e.g. a transmission to a same company data center located outside Colombia). Other processors add additional value to the data, under the instructions of the controller, but use the processors' own special processes. Lastly, a processor may simply provide processing resources at a remote location with the controller still the active processor of the data. Each circumstance would define the risk to Colombians from the transfer or transmission and the type of contractual mitigation required.

In the first and second instances, processing within the company and custom processing under the direction of the controller, there should be an intra-company contract or a contract with the external processor that specifies adherence to the policies established in Colombia. The third instance, the controller conducting processing within the domain of the processor, requires different contractual provisions. The contract should appropriately be limited to the types of risks associated with such processing. In this last instance, where the controller is conducting the actual processing, the risks to Colombians, resulting from the engagement of a third-party processor, are related to data security or the processor using the data for its own purposes. In that instance, the contract should specify the level of security to be maintained and prohibit the processor from using the data for its own purposes.

From a public policy perspective, it may seem reasonable to require a contract that obliges the processor to adhere to the privacy policy under which the data was collected or originated. However, such a requirement may make today's cloud services, no matter the geographic location, off limits for Colombian controllers. Cloud providers offer many different controllers with a safe place for the controllers to conduct their own processing. It may be very hard for a cloud provider, who is not providing custom, value added processing, to change basic storage services for each, individual controller. Therefore, I suggest that the contract should be specific to the risks.

I suggest SIC take two steps. First, I suggest SIC clarify that transfers to adequate countries require an appropriate level of due diligence that is no less than a transmission. Second, I suggest SIC clarify that controller contracts with third parties be specific to the risks associated with the processing.

As stated earlier, these are my personal comments, and they do not necessarily reflect the views of the IAF Board or its funders.

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

Sincerely,

Martin Abrams