

## **Laws of Puerto Rico Annotated**

Title 10 – Commerce

Subtitle 3 – Business Regulations Generally

Chapter 310 – Citizen Information of Data Banks Security Act

### **§ 4051. Definitions**

For the purposes of this chapter:

(a) *Personal information file.* Refers to a file containing at least the name or first initial and the surname of a person, together with any of the following data so that an association may be established between certain information with another and in which the information is legible enough so that in order to access it there is no need to use a special cryptographic code.

(1) Social security number.

(2) Driver's license number, voter's identification or other official identification.

(3) Bank or financial account numbers of any type with or without passwords or access code that may have been assigned.

(4) Names of users and passwords or access codes to public or private information systems.

(5) Medical information protected by the HIPAA.

(6) Tax information.

(7) Work-related evaluations.

Neither the mailing nor the residential address is included in the protected information or information that is a public document and that is available to the citizens in general.

(b) *Department.* Refers to the Department of Consumer Affairs.

(c) *Violation of the security system.* Means any situation in which it is detected that access has been permitted to unauthorized persons or entities to the data files so that the security, confidentiality or integrity of the information in the data bank has been compromised; or when normally authorized persons or entities have had access and it is known or there is reasonable suspicion that they have violated the professional confidentiality or obtained authorization under false representation with the intention of making illegal use of the information. This includes both access to the data banks through the system and physical access to the recording media that contain the same and any removal or undue retrieval of said recordings.

### **§ 4052. Notification**

Any entity that is the proprietor or custodian of a data bank for commercial use that includes personal information of citizens who reside in Puerto Rico must notify said citizens of any violation of the system's security when the data bank whose security has been violated contains all or part of the personal information file and the same is not protected by a cryptographic code but only by a password.

Any entity that as part of their operations resells or provides access to digital data banks that at the same time contain personal information files of citizens must notify the proprietor, custodian or holder of said information of any violation of the system's security that has allowed access to those files to unauthorized persons.

Clients must be notified as expeditiously as possible, taking into consideration the need of law enforcement agencies to secure possible crime scenes and evidence as well as the application of measures needed to restore the system's security. Within a non-extendable term of ten (10) days after the violation of the system's security has been detected, the parties responsible shall inform the Department, which shall make a public announcement of the fact within twenty-four (24) hours after having received the information.

#### **§ 4053. Notification--Character and method**

The notice of the violation of the system's security must indicate, as far as the need for any investigation or judicial case in course allows, the nature of the situation, the number of clients potentially affected, whether criminal complaints have been filed, what measures are being taken in the matter and an estimate of the time and cost required to rectify the situation. In case it is specifically known how the confidentiality of the information on an identifiable client was violated, said client shall be entitled to know which information was compromised.

To notify the citizens the entity shall have the following options:

(1) Written direct notice to those affected by mail or by authenticated electronic means according to the Digital Signatures Act.

(2) When the cost of notifying all those potentially affected according to subsection (1) of this section or of identifying them is excessively onerous due to the number of persons affected, to the difficulty in locating all persons or to the economic situation of the enterprise or entity; or whenever the cost exceeds one hundred thousand dollars (\$100,000) or the number of persons exceeds one hundred thousand [(100,000)], the entity shall issue the notice through the following two (2) steps:

(a) Prominent display of an announcement to that respect at the entities premises, on the web page of the entity, if any, and in any informative flier published and sent through mailing lists both postal and electronic, and

(b) a communication to that respect to the media informing of the situation and providing information as to how to contact the entity to allow for better follow-up. When the information is of relevance to a specific professional or commercial sector, the announcement may be made through publications or programming of greater circulation oriented towards that sector.

#### **§ 4054. No conflict with institutional information and security policies**

No provision of this chapter shall be interpreted as being prejudicial to those institutional information and security policies that an enterprise or entity may have in force prior to its effectiveness and whose purpose is to provide protection equal or better to the information on security herein established.

#### **§ 4055. Fines**

The Secretary may impose fines of five hundred dollars (\$500) up to a maximum of five thousand dollars (\$5,000) for each violation of the provisions of this chapter or its regulations. The fines provided in this section do not affect the rights of the consumers to initiate actions or claims for damages before a competent court.