**National Directorate for the Protection of Personal Data**

**Provision 11/2006**

**Approve the "Security Measures for the Treatment and Conservation of Data Personal Contained in Files, Registries, Banks and Public Databases not state and private ".**

Bs. As., 9/19/2006
Publication in BO: 9/22/2006

HAVING SEEN File No. 153.743 / 06 of the registry of the MINISTRY OF JUSTICE AND HUMAN RIGHTS, the powers attributed to this NATIONAL DIRECTORATE OF PROTECTION OF PERSONAL DATA by Law No. 25,326 and its regulations approved by Decree No. 1558 of November 29, 2001, and CONSIDERING:

That in accordance with the provisions of Article 9 of Law No. 25,326, the person responsible or The user of the data file must adopt the technical and organizational measures necessary to guarantee the security and confidentiality of personal data, in order to avoid its adulteration, loss, consultation or unauthorized treatment and that allow the detection deviations, intentional or not, of information, whether the risks come from the action human or technical means used.

That for its part, among the attributions assigned to the NATIONAL DIRECTORATE OF PROTECTION OF PERSONAL DATA is the one to dictate the norms and regulations that must be observed in the development of the activities included in the Law No. 25,326 (article 29, subsection 1, section b) and specifically that of issuing regulations administrative and technical procedures related to treatment and security conditions of public and private files, registries and databases or databases (article 29, paragraph 5, section a, of the Annex to Decree No. 1558/01), as well as that of controlling the observance of the rules on data integrity and security by files, records or banks of data (article 29, subsection 1, section d, of Law No. 25,326).

That as a consequence of this and in compliance with the faculty that this Control Body has for the issuance of rules relating to the security conditions of the files, registers and databases or databases, it corresponds to approve the security measures for the treatment and conservation of personal data, which must be observed by those responsible and users of public, non-state and private archives, registries, databases and databases.

That for this purpose, a "Personal Data Security Document" is established, such as instrument for the specification of safety regulations, which must be adapted in at all times to the current provisions on the matter dictated by the MANAGEMENT NATIONAL OF PERSONAL DATA PROTECTION.

That likewise, THREE (3) security levels are established: BASIC, MEDIUM and CRITICAL, according to the nature of the information processed, guidelines also applicable to files not computerized (manual registration).

That for each of the aforementioned levels, different measures of security, established taking into account the greater or lesser need to guarantee the confidentiality and integrity of the information contained in the respective database; the nature of the data and the correct management of the risks to which they are exposed, as well as well as the greater or lesser impact that the fact that the



information recorded in the files does not meet the integrity and reliability conditions due.

That different deadlines have been established for the implementation of the security measures that are promoted, taking into account the level of security in question, as well as the possibility of granting an extension upon duly substantiated request.

That the GENERAL DIRECTORATE OF LEGAL AFFAIRS of the MINISTRY OF JUSTICE AND HUMAN RIGHTS has taken the appropriate intervention

That this measure dictates the use of the powers conferred in article 29, paragraph 1, section b, of Law No. 25,326 and article 29, subsection 5, section a, of the Annex to Decree No. 1558/01.

Therefore, THE NATIONAL DIRECTOR OF PERSONAL DATA PROTECTION HAS:

Article 1 - Approve the "Security Measures for the Treatment and Conservation of The Personal Data Contained in Files, Registries, Banks and Public Databases are not State and Private ", the text of which as Annex I is part of this document.

Art. 2 - It is established that the deadline for the implementation of the security measures to be counted From the date of issuance of this act, it will be TWELVE (12) months for Basic Level, of TWENTY FOUR (24) months for the Medium Level and of THIRTY-SIX (36) months for those of Critical Level, which will be extendable at the request of the interested party and by duly founded reasons.

Art. 3 - Communicate, publish, give it to the NATIONAL REGISTRATION ADDRESS OFFICIAL and file. - Juan A. Naughty.

ANNEX I

"SECURITY MEASURES FOR THE TREATMENT AND CONSERVATION OF PERSONAL DATA CONTAINED IN FILES, RECORDS, BANKS AND BASES OF NON-STATE AND PRIVATE PUBLIC DATA "

• BASIC LEVEL SECURITY MEASURES:

Files, records, databases and databases that contain personal data must adopt the security measures classified as Basic Level that below Are detailed:

Have the Personal Data Security Document in which they are specified, between others, the procedures and security measures to be observed on the files, records, databases and banks that contain personal data. It must be kept at all times updated and be reviewed when changes occur in the information system.

It must contain:



1. Functions and obligations of the personnel.

2. Description of the files with personal data and the information systems that they treat them.

3. Description of the data control routines of the data entry programs and the Actions to follow in the event of errors detected for the purposes of their correction. All programs Data entry, whatever its processing mode (batch, interactive, etc.), must be include in its design, control routines, which minimize the possibility of incorporating into the illogical, incorrect or missing information, data.

4. Records of security incidents.

4.1. Notification, management and response to security incidents.

5. Procedures for making backup copies and data recovery.

6. Updated relationship between Information Systems and data users with authorization to its use.

7. Procedures for identification and authentication of data users authorized to use certain information systems.

The relationship between the authorized user and the information systems they can access it must be kept up to date. In the case where the authentication mechanism uses password, it will be assigned by the security officer according to a procedure that guarantees your confidentiality. This procedure should foresee the change periodical password (maximum period of validity) which must be stored in unintelligible way.

8. Control of user access to data and resources necessary to carry out their tasks for which they must be authorized.

9. Adopt preventive measures in order to prevent threats from malicious software (viruses, Trojans, etc.) that may affect files with personal data. Among other:

1) Install and update, with the relevant periodicity, software for detection and repair of virus, running it routinely; 2) Verify, before use, the absence of viruses in files received through the web, email and others whose origins are uncertain.

10. Procedure that guarantees an adequate Management of the Supports that contain data of personal nature (identification of the type of information they contain, storage in restricted access places, inventories, authorization to leave the premises where are located, destruction of disused information, etc.).

Note: When the files, registers, databases and banks contain a series of personal data with which, through a certain treatment, it is allowed to establish the profile of personality or certain behaviors of the person, the measures of security of the present level plus those established in points 2, 3, 4 and 5 of the following.

• MEDIUM LEVEL SECURITY MEASURES:



The files, registers, databases and databases of the private companies that develop public service provision activities, as well as files, registers, databases and banks of data belonging to entities that fulfill a public and / or private function that, beyond of the provisions of Article 10 of Law No. 25,326, they must keep the information secret personal by express legal provision (eg: bank secrecy), in addition to the measures of Basic level security, they must adopt the following:

1. The safety instructions must identify the person in charge (or specific body) of Safety.

2. Carrying out audits (internal or external) that verify compliance with the current procedures and instructions regarding security for personal data.

The pertinent audit reports will be presented to the Head of the Archive for the purposes that the corresponding corrective measures are adopted. The National Directorate of Protection of Personal Data, in the inspections you carry out, you must consider obligatorily, with a non-binding character, the results of the referred audits above, provided that they have been carried out within a maximum period one year.

3. The possibility of repeatedly attempting unauthorized access to the security system will be limited. information.

4. A physical access control will be established to the premises where the information systems with personal data.

5. Management of Supports and information contained therein, 5.1. A record of inputs and outputs of the computer media in order to identify the day and time of entry and output of the support, receiver, sender, shipping method, etc.

5.2. The necessary measures will be taken to prevent any recovery of the information after a medium is to be disposed of or reused, or that the information must be destroyed, for whatever reason.

Likewise, similar measures must be adopted when the supports, or the information (eg: When backup copies are made over a data transmission network, the information leaves a local support and travels to another remote via that network.), go out of the premises in which they are located, 5.3. There should be a procedure for the recovery of the supporting information and the treatment of the same in case of contingencies that put normal processing equipment (s) not operational.

6. The records of security incidents, in the case of having to recover data, must identify the person who retrieved and / or modified said data. Authorization will be required in reliable form of the person in charge of the computerized file.

7. The performance tests of the information systems, carried out prior to their operationalization will not be done with real data / files, unless the security levels corresponding to the type of computerized data processed.

• SECURITY MEASURES OF CRITICAL LEVEL:

The files, registers, databases and databases that contain personal data, defined as "sensitive data", with the exception that will be indicated below, in addition to the measures of Basic and Medium level security, they must adopt the following:



1. Distribution of supports: when distributing supports that contain files with data from personal character - including backup copies - such data must be encrypted (or used any other mechanism) in order to guarantee that they cannot be read or manipulated during his transport.

2. Access register: there must be an access register with information that Identify the user who accessed, when he did it (date and time), type of access and if it has been authorized or denied. In the event that access has been authorized, the data accessed and the treatment given to it (cancellation, rectification, etc.). This record of accesses must be periodically analyzed by the security officer and must be kept as a kitten for a term of THREE (3) years.

3. Backup copies: in addition to those that are kept in the location where the data should be implemented external backup copies, located outside the location, in fireproof and gas-proof box or in a bank safe, any of them located at a reasonable distance from the aforementioned location. There should be a procedure for the recovery of this information and its treatment in case of contingencies that render the usual processing equipment (s) inoperative.

4. Data transmission: personal data that is transmitted through networks of communication1, they must be encrypted or using any other mechanism that prevents their reading and / or treatment by unauthorized persons.

Note: Files, files, registries, databases and databases that must carry out the processing of sensitive data for the purposes administrative or legal obligation. However, this does not exclude that they should also have those safeguard measures that are necessary and appropriate to the type of data.