National Bureau for the Protection of Personal Data

Provision 11/2006

The "Security Measures for the Treatment and Maintenance of the Personal Data Contained in Files, Records, Databanks and Databases, either non state Public and Private" be passed.

Bs. As., 9/19/2006
Publication in the Official Gazette: 9/22/2006

IN VIEW OF File No 153,743/06 of the registry of the MINISTRY OF JUSTICE AND HUMAM RIGHTS, the responsibilities ascribed to the NATIONAL BUREAU FOR THE PROTECTION OF PERSONAL DATA by Act No 25,326 and establishment thereof by Decree 1558 of November 29 2001, and

CONSIDERING,

That in conformity with the provisions of section 9 Act 25,326, the responsible for, or the user of, the data file shall adopt such technical and organization measures as needed to ensure the security and confidentiality of the personal data, in order to avoid its adulteration, loss, non- authorized consultation and treatment and to allow to pinpoint any information deviations, either intentional or not, whether the risks arise from human action or from the technical means used.

That, in turn, among the powers assigned to the NATIONAL BUREAU FOR THE PROTECTION OF PERSONAL DATA there is the responsibility of issuing rules and regulations that must be complied with in the development of the activities encompassed in Act 25,326 (section 29, subsection 1, paragraph b), and specifically the responsibility of issuing administrative rules and technical procedure rules related to the treatment and security conditions of the files, record and databases or databanks, both public and private (section 29, subsection 5, paragraph a, Annex to Decree 1558/01), as well as that of supervising observance of the rules on data integrity and security by the files, records or databanks (section 29, subsection 1, paragraph d, Act 25,326).

That, as a consequence of the above and in compliance with the powers that this Controlling Entity has for issuing the rules relative the security conditions of files, records and databases or databanks, it is to approve the security measures for the treatment and maintenance of personal data which shall be complied with by those responsible for, and the users of non-state public and private files, records, databases and databanks.

That to such purpose, it is established a "Personal Data Security Document" as an instrument for specifying the security rule, which shall adapt at every time to the regulations in force on this regard as issued by the NATIONAL BUREAU FOR THE PROTECTION OF PERSONAL DATA.

Further, that THREE (3) security levels are set: BASIC, MID and CRITICAL, according to the type of the information dealt with, including guidelines also applicable to the non computerized files (manual recording).

That, for each of the above mentioned levels several security measures have been provided and established, by taking into account the larger or lesser need for ensuring the confidentiality and integrity of the information contained in the relevant databank, the type of the data and the adequate management of the risks they are exposed to, as well as the higher or lower impact on individuals by the fact that the information recorded in the files do not meet the due integrity and reliability conditions.

That different terms have been established for the implementation of the security measures advocated, taking into account the level of security involved, as well as the possibility of obtaining an extension after the appropriate request has been filed.

That THE NATIONAL BUREAU OF LEGAL AFFAIRS OF THE MINISTRY OF JUSTICE AND HUMAN RIGHTS has become involved as being incumbent upon.

That this measure is issued on the basis of the faculties granted under section 29, subsection 1, paragraph b of Act 25,236 and section 9, subsection 5, paragraph a, of Annex to Decree 1558/01.
have intervened as being incumbent upon.

Consequently,

THE NATIONAL DIRECTOR OF PROTECTION OF PERSONAL DATA BUREAU

PROVIDES:

Section 1 — The "Security Measures for the Treatment and Maintenance of the Personal Data Contained in Files, Records, Databanks and Databases, either non state-owned Public and Private" be passed, the text of which is an integral part hereof as Annex I.

Section 2 — That the term for the implementation of the security measures to run as of the date of issue hereof, shall be TWELVE (12) months for Basic Level measures, TWENTY-FOUR(24) months for Mid Level measures and THIRTY-SIX (36) months for Critical Level measures, which shall be extendable upon the request of the party concerned and on duly grounded reasons.

Section 3 — Let it be communicated, published, and delivered to the NATIONAL REGISTRY and duly filed in the Archive. — Juan A. Travieso.

ANNEX I

"SECURITY MEASURES FOR THE TREATMENT AND MAINTENANCE OF THE PERSONAL DATA CONTAINED IN FILES, RECORDS, DATABANKS AND DATABASES, EITHER NON STATE-OWNED PUBLIC AND PRIVATE"

*SECURITY MEASURES BASIC LEVEL:

The files, records, databases and databanks containing personal data shall adopt such security measures as classified as Basic Level which are herein below indicated:

To have available the Personal Data Security Document including the security procedures and measures to be abode by on the files, records, databases and databanks containing personal data. It shall be kept at every time updated and reviewed whenever any changes to the information system are made.

It shall contain:
1. Responsibilities and duties of staff.

2. Description of the files with personal data and the information systems handling them.

3. Detail of all the routines of data control of the data entry programs and the steps to follow in view of the errors found for them to be corrected. All the data entry programs, whatever its processing mode may be (batch, interactive, etc) shall include in their design, control routines to minimize the possibility of incorporating illogical, incorrect or missing data to the information system.

4. Records of security faults (incidents).

4.1. Reporting, management and feedback in view of security incidents.

5. Procedures on creation of data backup and recovery files.

6. Updated relation between Information systems and data users authorized to the use thereof.

7. Procedures on identification and authentication of data users authorized to use certain information systems. The relation between the authorized user and the information systems he may access shall be kept updated. In the case the authentication mechanism uses a password, it shall be assigned by the person responsible for the security according to a procedure which ensures the confidentiality thereof. This procedure shall foresee the periodical password change (maximum duration term) which shall be stored in an unreadable manner.

8. Control of user access to data and resources needed for job performance to which they must be authorized.

9. To adopt prevention measures in order to prevent malicious software threats (virus, troyans, etc.) that may affect files with personal data. Including: -

1) To install and update, with the relevant frequency, virus detection and repair software, by running it on a routine basis; 2) To check, before its use, the inexistence of virus in files received via internet, email, the origin of which is uncertain.

10. Procedure that ensures an adequate Support Management containing personal data (identification of the type of information they contain, storage in restricted access places, inventories, authorization for their being taken out of the premises they are placed at, destruction of disuse data, etc.).

Note: When the files, record, databases and databanks contain a series of personal data enabling, through certain handling, to set the individual's personality profile or certain behaviors, the security measures of this level plus those set forth in items 2, 3, 4 and 5 hereof shall be ensured.

*SECURITY MEASURES MID LEVEL:

Private companies' files, records, databases and databanks of private companies which provide utilities services such as files, record, databases and databanks which belong to entities that have a public and/or private purpose that, beyond the provisions of section 10 Act 25,236, must keep secrecy of the personal data by express legal provision (eg. bank secret), shall adopt the measures as indicated herein below in addition to the Basic level security measures, as follows:-

1. The Responsible (or specific entity) for Security shall be identified in the Security Instructions.

2. Audits (internal or external) to check the performance of the procedures and instructions in force regarding personal data safeguarding.

The relevant audit reports shall be submitted to the Responsible for File for the relevant correcting measures to be adopted. The National Bureau of Personal Data Protection, in the inspections it will carry out, shall compulsorily consider on a non-binding basis the results of the above-mentioned audits, provided they have been performed with a maximum term of one year.

3. Repeated attempt of non-authorized access to the information system shall be limited.

4. A physical access control to the premises where the information systems containing personal data are placed shall be established.

5. Support Management and information contained thereof.

5.1. It shall be established an input/output record of the computing support to identify day and time of input/output of support, receiver, sender, sending form, etc.

5.2. The required steps to prevent any recovery of information after a support is rejected or reused, or any information from being destroyed by any cause whatsoever shall be taken.

Further, similar measures are to be taken when the supports or the information (eg. when backup files are made through a data transmission network, the information exits a local support and travels to another remote via said network) is going to exit outside of the premises they are placed in.

5.3. A recovery procedure of backup and treatment thereof shall be available in the case of any contingency that may render non-operative the usual processing equipment(s).

6. The security fault register, in the case that recovery is needed, shall identify the individual who recovered and/or changed said data. The due authorization by the responsible for the computerized filed shall be required.

7. The service test of the information systems, performed in advance of their putting in service shall not be performed with actual data/files, unless the security levels for the type of computerized data treated are ensured.

*SECURITY MEASURES CRITICAL LEVEL:

The files, records, databases and databanks containing personal data, defined as "sensitive data", save for the exception as indicated herein below, in addition to the Basic and Mid Level security measures, shall adopt such measures as herein below listed: -

1. Support distribution: when supports containing personal data files – including the backup files – are distributed, those data shall be coded (or else, any other mechanism shall be used) in order to ensure they cannot be read or handled during their transport.

2. Access record: An access record with information identifying the user accessing it, when (data and time), type of access and whether it has been authorized or rejected shall be available. In the case that the access has been authorized the accessed datum and the treatment given to it shall be identified (drop, rectification, etc). This access record is to be frequently analyzed by the responsible for security and is to be maintained at least for THREE (3) years.

3. Backup files: in addition to those maintained in the location where data reside, external backup files are to be implemented, and to be placed outside of the location in fire-proof, gas boxes, or else in a bank safety box, any of them placed at a reasonable distance from said location. A recovery procedure of backup and treatment thereof shall be available in the case of any contingency that may render non-operative the usual processing equipment(s).

4. Data transmission: Personal data transmitted through the communication networks shall be coded, or else, any other mechanism shall be used in order to avoid their being read and/or handled by nonauthorized individuals.

Note: The files, records, databases and databanks which shall handle sensitive data for administrative or legal purposes, are released from applying the critical level security measures. However, the above does not preclude that they shall take such backup measures as needed and suitable to the type of information.