National Directorate for the Protection of Personal Data

PERSONAL DATA PROTECTION

Provision 9/2008

Security Measures for the Treatment and Conservation of Personal Data Contained in Files, Registries, Banks and Public Non-State and Private Databases. Extend the deadline established by Provision No. 11/2006.

Bs. As., 9/1/2008

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 PERSONAL DATA PROTECTION by Law No. 25.326 and its regulations approved by Decree No. 1558 of November 29, 2001, and

CONSIDERING:

That by DNPDP Provision No. 11, dated September 19, 2006, the "Security Measures for the Treatment and Conservation of Personal Data Contained in Files, Registries, Banks and Non-State Public Databases and Private ".

That also different deadlines were established for the entry into force of the security measures according to the fact that, due to the nature of the information processed, it would be appropriate to adopt those of Basic, Medium or Critical Level.

That it was determined that after TWELVE (12) months of entry into force of the aforementioned provision, the Basic Level Security Measures would be mandatory, as well as that at TWENTY-FOUR (24) months the same would occur with the Medium Level and the THIRTY-SIX (36) months with the Critical Level.

That the rule provides for the extension of such terms at the request of the interested party and for duly founded reasons.

That on September 22 of this year the Medium Level Security Measures will come into effect.

That having observed that the Basic Level Security Measures have not yet been adequately internalized, it is convenient to extend the period of entry into force of the Medium and Critical Levels in general, so that the Requirements contemplated in the Medium Level are required only within TWELVE (12) months and those of Critical Level as of TWENTY-FOUR (24) months, in both cases counted from the date hereof.

That the aforementioned provision also established that the files, registers, databases and personal data banks should have a "Personal Data Security Document", in which the applicable security regulations were specified.

That in order to facilitate the implementation of the aforementioned document and the effective implementation of technical measures that guarantee security and confidentiality in the processing of personal data, it is appropriate to promote from this Body of Control a Security Document Model that contains essential minimum guidelines that allow the obligated parties to design an instrument that is adapted to the needs of their organization and complies with the regulations issued on the matter.

That the need to propose a "Security Document" text is based on the fact that difficulties have been noticed in the preparation of the aforementioned document by some managers and users of personal databases.

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

That this measure is issued in use of the powers conferred in article 29, subsection 1, section b, of Law No. 25.326 and article 29, subsection 5, sections a and e, of the Annex to Decree No. 1558/01.

Thus,

THE NATIONAL DIRECTOR OF PERSONAL DATA PROTECTION

HAS:

Article 1 - Extend the term established by DNPDP Provision No. 11/06 for the implementation of the security measures of the Medium and Critical Levels, which will be required within TWELVE (12) and TWENTY-FOUR (24) months, respectively, counting from the entry into force of this act. Said period will be extendable at the request of the interested party and for duly founded reasons.

Art. 2 - Approve the "Personal Data Security Document", which as Annex I is an integral part of this.

Art. 3 - Communicate, publish, give to the National Directorate of the Official Registry and file. - Juan A. Naughty.

ANNEX I

PERSONAL DATA SECURITY DOCUMENT

_____

Responsible for the Data : (name of the firm / organization)

CUIT: (CUIT of the firm)

Address: (street - N° - floor / office - Post code - City - Province)

Phone: No. **Email:**

Registration in the National Registry of Data Banks N° : (indicate registration number)

Date of the last Renewal : dd / mm / yy *Valid for ONE year.*

Contact person of the firm / organization : (name, surname and contact information)

_____

Responsible for security management at the firm : (name and surname)

Category / Hierarchy / Rank:

CUIT or CUIL : (CUIL of the person in charge)

_____

Revision and application date : dd / mm / yy

Maturity: dd / mm / yy

_____

Scope:

These security measures are defined as BASIC LEVEL, a minimum that can be improved; and they apply to the information consigned in the inscriptions made in the DNPDP, and to its management systems (programs, files, tasks contracted, etc.).

Its purpose is to maintain the integrity, accessibility and confidentiality of personal data, and they are reviewed and / or updated at least once a year.

1- Functions and obligations of the personnel or contractors.

All staff and / or suppliers with access to personal data are properly informed and undertake to observe strict confidentiality of the information held by the company through the signature of a "Confidentiality Obligation" such as the one transcribed, or similar.

Obligation of confidentiality: The one who subscribes.... (first name last name, CUIT-CUIL)..., employee (or provider with access to the data), assumes the commitment to maintain strict secrecy and confidentiality of the information accessed, not having to externalize it partially or totally without authorization. I hereby notify myself of the confidential nature of the information held by the person responsible for the data and I agree not to use or disclose it without their consent. Personal information present, their manipulation, treatment, assignment or disclosure are protected and regulated by Law No. 25.326 of Habeas Data (http://www.jus.gov.ar/datospersonales/pdf/ley_25326.pdf), being the Management National Protection of Personal Data, of the Ministry of Justice, Security and Human Rights, the Control Body of the aforementioned legal norm (http://www.jus.gov.ar/datospersonales/).

Profiles can be defined as Boss or Secretary, if the firm has them, and assign to each profile, obligations and "privileges". There can be several employees under the same profile.

Boss, Managing Partner, President or owner of the studio, factory, business.

Obligations: head of the company with maximum responsibility, assignment of responsibilities to subordinates, tasks, limitations.

Secretary

Obligations: keep updated agendas, assign shifts, invoice, collect, others specify **.**

Administrative employee

Obligations:

- Operate the system, book, request purchases, issue invoices, collect, settle salaries.

- Keep information safe by making backups, accounting and storing backups under lock and key, keeping the administration area closed, running anti-virus update routines.

- Others (specify.

External provider and systems service (Enter name and CUIT)

Obligations:

- Maintain information systems working properly while maintaining the integrity of personal data.

- Access all the information that the company stores in its systems.

- Others (specify

2- Description of the files with personal data and the systems that process them

List of clients, list of suppliers, list of personnel, others to specify.

Administrative management program brand and version specify is used.

Operating system brand and version specify.

3- Description of the data control routines and actions to follow in the event of errors.

The personnel involved are instructed to perceive possible inconsistencies or errors and correct them as soon as they take account if the system allows it, or notify the appropriate person with the possibility of correcting them.

4- Records of security incidents. Notification, management and response.

A DNPDP folder is created in the email program, and then all emails referring to personal data protection are passed to it.

When something happens that is considered a security incident, one or more emails are written describing what happened and the actions taken to solve it, and they are sent to another account.

In this way, the dates and times, the characteristics, and the solution of the incident are recorded in those emails.

You can also keep a record of incidents in a chapter of a System Report Notebook where all the events related to the Protection of Personal Data are reported, which is kept under lock and key in the Secretary's desk.

5- Procedure to carry out backup copies and data recovery (Backups)

The Documents and.... (specify others) ... folders are copied to two CD ROMs, and the correct copying is verified with the copy program routine, as well as reading them.

The date and the folders that have been copied to it are recorded on the surface of the CDs.

A CD is kept under lock and key in a cabinet in the administration office and another is taken to the home address of the owner of the firm.

6- Updated relationship between Information Systems and Data Users.

Data Users are all those who use the data stored by the firm: administrative employees, secretaries, vendors, etc.

Not always any employee can access any data or function, the privilege to access such or which data or functions are granted to each profile: "Boss", "Secretary", "1st Administrative", "2nd Administrative", etc.

This Relationship between Systems and Users is consistent with the "privileges" of each profile.

Boss, Managing Partner, President or owner of the studio, factory, business.

YES Access to: all company information.

Secretary

YES Access to: Everything except what is specified in NO.

NO Access to: personnel files, others specify.

Administrative (includes all administrative in general).

YES Access to: customized for each sub-profile.

NO Access to: customized for each sub-profile.

Administrative 1st General, Personal

YES Access to: information on clients, suppliers, staff, Internet, others specify

NO Access to: Chief's personal agenda, others specify.

Administrative 2nd Purchases, Sales

YES Access to: information on customers, suppliers, Internet, others specify

NO Access to: Chief's personal agenda, personnel files, others specify

Provider of computer systems, or documentation or data archiving.

YES Access to: all company information with limitations and obligations described in the service contract and / or the "Obligation of confidentiality".

7- Procedures for identification and authentication of data users.

The system has unique "User Accounts", which are assigned to each person who accesses it.

Each account has a secret "*password*", only known by the user, which is required to authenticate and access the system.

The password has no less than eight characters and must be changed by the user every 30 days as it expires automatically.

8- Access control of data users.

According to their "profile", keys are assigned to the entrance doors to each sector of the firm.

Furniture and drawers with particular keys are assigned to each User.

In the computer system, each User has an account with his "password", and with his particular "privileges" of access to certain information.

9- Prevention measures against malicious software threats.

The operating system has a "Security Module" with Firewall to prevent unwanted access by intruders through the Internet, and memory resident Antivirus program that limits the entry of viruses through networks, floppy disks, CDs or others. input devices.

This "Security Module" has a periodic and automatic update request, which is carried out each time it occurs.

10- Procedure that guarantees the adequate Management of the Data Carriers.

Backup data carriers, eg. Backup CD ROMs are labeled indicating, date, and contents in general.

The backup is recorded in a chapter that contains the Systems Report Notebook, where they copy what is written on the CD label.

An email is written with the same content, it is sent to another account and it is passed to the previously created DNPDP folder.

A CD is kept under lock and key in a cabinet in the administration office and another is taken to the home address of the firm.

When the information on a data medium is no longer useful and has been prescribed, it will be destroyed, scratching its surface and breaking it into pieces before throwing it away.

The transaction entry is made in the Systems Report Notebook, and in the email.

Firm	Firm
Responsible for Personal Data	Security Manager
DNI - CUIT	DNI - CUIT - CUIL