Bill No. [handwritten:] 4019/2009-[illegible]

[stamp:]
CONGRESS OF THE REPUBLIC
DOCUMENT PROCESSING AREA
JUNE 9, 2010
RECEIVED
Signature Time: [hw:] 8:00 p.m.

"Decade of the Persons with Disabilities in Peru"
"Year of Peru's economic and social consolidation"

Lima, June 09, 2010

LETTER No. 128-2010-PR

Doctor
LUIS ALVA CASTRO
President of the Congress of the Republic
By Messenger.-

We are pleased to write, pursuant to article 107 of the Political Constitution of Peru to submit for the consideration of the Congress of the Republic, with the approval vote of the Council of Ministers, the Bill for Personal Data Protection.

We would appreciate it if you see to it that it is processed urgently, pursuant to Article 105 of the Political Constitution of Peru.

Without other particulars, we take this opportunity to renew our sentiments of esteem and consideration.

Sincerely,

[signature]
ALAN GARCÍA PÉREZ
Constitutional President of the Republic

[signature]
JAVIER VELÁZQUEZ QUESQUÉN
President of the Council of Ministers

CONGRESS OF THE REPUBLIC
Lima, [handwritten:] June 14, 2010
According to the consultation conducted pursuant to Article 77 of the Regulation of the Congress of the Republic: Proposal No. [handwritten:] 4079 was passed. For study and opinion to the Commission(s) of [handwritten:] Justice and Human Rights.

[signature]
JOSE ABANTO VALDIVIESO
Secretary (e)
CONGRESS OF THE REPUBLIC

[handwritten]

REPUBLIC OF PERU
[seal]

Bill

LAW FOR PERSONAL DATA PROTECTION

TITLE I

GENERAL PROVISIONS

Article 1.- Object

The object of this Law is to guarantee the fundamental right to personal data protection provided in article 2, paragraph 6 of the Political Constitution of Peru through their adequate processing, within a framework of respect for the other fundamental rights recognized therein, especially the rights to honor, good reputation, privacy, speech and image.

Article 2.- Definitions

For all purposes of this Law, the following will have the meaning indicated:

2.1 Personal data database.- Organized set of personal data, automated or not, regardless of the medium, be it physical, magnetic, digital, optical or others to be created, regardless of the form or modality of their creation, formation, storage, organization and access.

2.2 Privately administered personal data database.- Personal data database held by an individual or a private legal person if the database is not strictly related to the exercise of public law powers.

[handwritten]

2.3 Publicly administered personal data database.- Personal data database held by a public entity.

2.4 Personal data.- Any information on an individual which identifies or makes him identifiable through means that may be reasonably used.

2.5 Sensitive data.- Personal data consisting of biometric data, data concerning the racial and ethnic origin; political, religious, philosophical or moral opinions or convictions, personal habits, union membership and information related to health or sexual life.

2.6 Personal data database processor.- Any individual, private legal person or public entity which alone or jointly with others, processes the personal data at the order of the personal data database controller .

2.7 Public entity.- Entity included in article I of the Preliminary Title of Law No. 27444, Law of General Administrative Procedure or its replacement.

2.8 Trans-border Personal Data Flow.- International transfer of personal data to an addressee located in a country other than the country of origin of the personal data, regardless of the media on which they are found, the means by which the transfer was made or the processing they receive.

2.9 Sources accessible to the public.- Personal data databases publicly or privately administered, which may be consulted by any person after paying the corresponding fee, if applicable. The sources accessible to the public will be determined in the regulation.

2.10 Private legal person.- For the purposes of this Law the legal person not included within the scope of article I of the Preliminary Title of Law No. 27444, Law of General Administrative Procedure.

2.11 Anonymization procedure.- Processing of personal data that prevents the identification or does not make the data subject identifiable. The procedure is irreversible.

[handwritten]

2.12 Dissociation procedure.- Processing of personal data that prevents the identification or does not make the subject identifiable. The procedure is reversible.

2.13 Data subject.- Individual to whom the personal data belong.

2.14 Personal data controller.- Individual, private legal person or public entity that determines the purpose and content of the personal data database, their processing and the security measures.

2.15 Personal data transfer.- Any transmission, supply or expression of personal data, national or international in character, to a private legal person, a public entity or an individual other than the data subject.

2.16 Personal data processing.- Any operation or technical procedure, automated or not, that allows compiling, registration, organization, storage, conservation, preparation, modification, extraction, consultation, utilization, blockage, suppression, communication by transfer or distribution or any other form of processing that facilitations the access, correlation or interconnection of the personal data.

The regulation of this Law may establish other definitions and/or expand existing ones.

Article 3.- Scope of application

This Law applies to the personal data contained or intended to be contained in personal data databases publicly and privately administered, processed in the national territory. Sensitive data are the object of special protection.

The provisions of this law will not apply to the following personal data:

3.1 Those contained or intended to be contained in personal data databases created by individuals for purposes exclusively related to their private or family life.

3.2 Those contained or intended to be contained in publicly administered databases, only to the extent that their processing is necessary for strict

compliance with the powers assigned by law to the respective public entity for national defense, public security, the development of activities in criminal matters for the investigation and repression of crime.

TITLE II

GUIDING PRINCIPLES

Article 4.- Principle of legality

The processing of the personal data will be done according to the provisions of the law. Compiling personal data by fraudulent, unfair or illegal means is prohibited.

Article 5.- Principle of consent

The data subject must give his consent for the processing of personal data.

Article 6.- Principle of purpose

Personal data must be compiled for a determined, explicit and legal purpose. Personal data processing must not be extended to a purpose other than that established unequivocally as such at the time of compiling, excluding the cases of activities with historical, statistical or scientific value when using a dissociation or anonymization procedure.

Article 7.- Principle of proportionality

Any personal data processing must be adequate, relevant and non-excessive for the purpose for which the data were compiled.

Article 8.- Principle of quality

Personal data to be processed must be truthful, accurate and, as far as possible, updated, necessary, pertinent and adequate for the purpose for which they were compiled. They must be kept so as to guarantee their security and only for the time necessary to achieve the purpose of the processing.

Article 9.- Principle of security

The personal data database controller and the data processor must adopt the necessary technical and organizational measures to guarantee the security of the personal data. Security measures must be

appropriate and in line with the processing to be done and the category of personal data in question.

Article 10.- Principle of availability of recourse

Any data subject must have the administrative and/or jurisdictional channels necessary to claim and enforce his rights when they are violated by the processing of his personal data.

Article 11.- Principle of adequate level of protection

In the case of trans-border personal data flow, the receiving country must have a sufficient level of protection for the personal data to be processed or at least comparable to that provided by this Law.

The sufficient protection scope of the receiving country must include at least the consignment and compliance with the guiding principles of protection of the personal data under this Title and an effective system of guarantees.

Article 12.- Values of the principles

The acts of the controllers and processors of personal data databases and in general all those intervening in connection with personal data must comply with the guiding principles referred to in this Title. This list of guiding principles is not limited thereto.

The guiding principles indicated will also serve as interpretation criterion to resolve the issues that may arise from the application of this Law and this regulation as well as a parameter for the preparation of other provisions and to fill gaps in the law in the matter.

TITLE III

PERSONAL DATA PROCESSING

Article 13.- Scope of processing

13.1 Personal data processing must be done in full respect of the fundamental rights of the subjects and the rights granted to them by this Law. The same rule governs their use by third parties.

13.2 The limitations to the exercise of the fundamental right to the protection of personal data may be established only by law in accordance with their essential content and be justified by the respect of other fundamental rights or constitutionally protected assets.

13.3 Special measures will be enacted by regulation for the processing of the personal data of children and adolescents as well as for the protection and guarantee of their rights. For the exercise of the rights recognized by this Law, children and adolescents will act through their legal representatives whereby the regulation may determine the applicable exceptions, if appropriate, taking into account the superior interest of the child and adolescent.

13.4 Communications, telecommunications, computer systems or their instruments, when they are of a private character or use, may be opened, seized, intercepted or audited only by motivated order of the judge or with the authorization of their subject, with the guarantees provided in the law. Secrecy is kept concerning the matters unrelated to the fact that motivates their examination. The personal data obtained in violation of this precept are devoid of legal effect.

13.5 Personal data may be processed only with the consent of the subject, except in case of authoritative law in this regard. The consent must be prior, informed, express and unequivocal.

13.6 In the case of sensitive data, the consent for processing must also be given in writing. Even without the consent of the subject, the processing of sensitive data may take place when authorized by law provided that it obeys important reasons of public interest.

13.7 The data subject may revoke its consent at any time with the obligation to support his request when applicable, complying in this regard with the same requisites as when he gave his consent.

13.8 The processing of personal data concerning the perpetration of criminal or administrative violations may only be done by the competent public entities, except in case of management agreement pursuant to Law No. 27444, Law of General Administrative Procedure or its replacement. In case of cancellation of the criminal judicial police and administrative record, these data may not be disclosed unless they are required by the Judiciary or the Prosecutor's Office, pursuant to the Law.

13.9 The marketing of personal data contained or intended to be contained in personal data databases is subject to the provisions of the regulation of the Law.

[handwritten]

Article 14.- Limitations to consent for personal data processing

The consent of the data subject will not be required for processing in the following cases:

14.1 When the personal data are compiled or transferred for the performance of the functions of the public entities within their competence.

14.2 In case of personal data contained or intended to be contained in sources accessible to the public.

14.3 In case of personal data related to financial solvency and credit, pursuant to the Law.

14.4 In case of a law for the promotion of competition in regulated markets issued in the performance of the regulatory function by the regulatory entities referred to in Law No. 27332, Framework Law of Regulatory Entities of Private Investment in Public Services or its replacement, provided that the information contributed is not used in violation of the user's privacy.

14.5 When the personal data are necessary to perform a contract to which the data subject is a party.

14.6 In case of personal data related to health and, if they are necessary, under risk circumstances, for the prevention, diagnosis and medical or surgical treatment of the data subject, provided that such treatment is carried out by health establishments or health science professionals, observing professional secrecy; or in case of reasons of public interest provided by Law; or if they must be processed for reasons of public health or to conduct epidemiological or similar studies, provided that adequate dissociation procedures are applied.

14.7 When the processing is carried out by not for profit organizations with political, religious or union purposes, and refers to the compiled personal data of their respective members, in which case the data must be related to the purpose of their activities and may not be transferred without the consent of the members.

14.8 In case of application of an anonymization or dissociation procedure.

14.9 Others established by Law.

Article 15.- Trans-border flow of personal data

The data controller and the data processor of the personal data database may engage in transport the flow of personal data only if the recipients keep adequate protection levels according to this Law. The National Authority for the Protection of Personal Data will supervise compliance with this requirement.

The provisions of the previous paragraph do not apply in the following cases:

15.1 Agreements under international treaties on the matter to which the Republic of Peru is a party.

15.2 International judicial cooperation.

15.3 International cooperation between intelligence agencies for the fight against terrorism, illegal drug trafficking, money laundering, corruption, human trafficking and other forms of organized crime.

15.4 When the personal data are necessary to implement a contract to which the data subject is a party.

15.5 In case of bank or stock exchange transfers, concerning the respective transactions according to the applicable Law.

15.6 When the trans-border flow of personal data takes place for the prevention, diagnosis or medical or surgical treatment of the data subject; or when it is necessary to carry out epidemiological or similar studies, provided that adequate dissociation procedures are applied.

15.7 When the data subject has given his prior, informed, express and unequivocal consent.

15.8 Others established by regulation of this Law.

Article 16.- Security

For purposes of personal data treatment, the data controller must adopt technical, organization and legal measures to guarantee their security and avoid their alteration, loss, unauthorized processing or access.

[handwritten]

The requisites and conditions to be met by personal data databases in matters of security will be established by the National Authority for the Protection of Personal Data.

It is prohibited to process personal data in databases that do not meet the requisitions and security conditions referred to in this article.

Article 17.- Confidentiality

The data controller, the data processor and the persons participating in any part of their processing are obligated to keep confidentiality concerning the data and their background. This obligation will survive even after the termination of the relationship with the data controller.

The obligor may be relieved from the confidentiality obligation in case of prior, informed, express and unequivocal consent of the data subject, consensus or final judicial decision, or in case of founded reasons concerning the national defense, public security or public health, without prejudice to the right to keep professional secrecy.

TITLE IV
RIGHTS OF THE DATA SUBJECT

Article 18.- Right to information

The data subject has the right to be informed in detail, simply, expressly, unequivocally and prior to compiling, about the purpose for which his personal data will be processed; who will be or who may be the recipients, the existence of the database in which they will be stored, as well as the identity and address of the controller and, if applicable, the processor of his personal data; the mandatory or optional character of his answers to the questionnaire proposed to him, especially concerning sensitive data; the transfer of personal data; the consequences of providing his personal data and of his refusal to do so; the time during which his personal data will be kept; and the possibility to exercise the rights granted to him by law.

If the personal data are collected online through electronic communication networks, the obligations of this article may be met by publication of privacy policies, which must be easily accessible and identifiable.

Article 19.- Right of access

The data subject has the right to obtain information processed about him in publicly or privately administered databases, the way his data were compiled, the reasons for their compiling and at whose request the compiling was done, as well as the transfers made or planned to be made of such data.

Article 20.- Right of update, inclusion, rectification and elimination

The data subject has the right to the update, inclusion, rectification and elimination of his personal data processed when they are partially or totally inaccurate, incomplete, when noticing omission, error or inaccuracy, when they are no longer necessary or relevant for the purpose for which they were compiled or upon the expiration of the term established for their processing.

If his personal data were previously transferred, the personal data database controller must communicate the update, inclusion, rectification and/or elimination to the party to whom they were transferred, if the latter continues processing them, and the latter must also proceed with the update, inclusion, rectification and/or elimination, as the case may be.

During the process of update, inclusion, rectification and/or elimination of personal data, the personal data database controller will order their blockage, being prohibited from allowing third parties to access them.

The elimination of personal data contained in publicly administered personal data databases is subject to the provisions of article 21 of the Sole Amended Text of Law No. 27806, Law of Transparency and Access to Public Information or its replacement.

Article 21.- Right to prevent the supply

The data subject has the right to prevent the data from being supplied, especially when it affects his fundamental rights.

Article 22.- Right of opposition

Provided that it is not otherwise set forth in the law and in the absence of consent, the data subject may oppose their processing when he has founded and legitimate reasons related to a concrete personal situation. In case of justified opposition, the controller or processor of the personal data database, as the case may be, must eliminate them, pursuant to the law.

[handwritten]

Article 23.- Right to objective processing

The data subject has the right not to be subjected to a decision with legal effects on him or affecting him significantly, supported only by a processing of personal data intended to evaluate certain aspects of his personality, unless it occurs within the negotiation, execution or performance of a contract or in cases of evaluation with purposes of incorporation into a public entity, pursuant to the law, without prejudice to the possibility of defending his point of view for the protection of his legitimate interest.

Article 24.- Right to protection

If the controller or processor of the personal data database denies the data subject in full or in part the exercise of his rights established in this Law, he may appear before the National Authority for Personal Data Protection, lodging a complaint, or to the Judiciary for the purposes of the corresponding action of habeas data.

The procedure to be followed with the National Authority for Personal Data Protection is subject to articles 219 et seq. of Law No. 27444, Law of General Administrative Procedure, or its replacement.

The resolution of the National Authority for Personal Data Protection exhausts the administrative channel and allows for the imposition of the administrative sanctions provided in article 39 of this Law. The regulation will determine the corresponding instances.

The resolutions of the National Authority for Personal Data Protection may be opposed by administrative-litigation action.

Article 25.- Right to be indemnified

The data subject affected as a consequence of the violation of this Law by the controller or processor of the personal data database or by third parties has the right to obtain the corresponding indemnity according to the law.

Article 26.- Free of charge character

No fee will be required from the data subject for the exercise of the rights contemplated in articles 19, 20, 21, 22 and 23 of this Law, except in the cases established by the regulation.

Article 27.- Limitations

The controllers and processors of publicly administered databases may deny the exercise of the rights of access, update, inclusion, rectification, elimination and opposition for reasons based on the protection of the rights and interests of third parties or where it can prevent pending judicial or administrative proceedings related to the investigation of the compliance with tax or social security obligations, the performance of health and environmental control functions, the verification of administrative violations or when so ordered by law.

TITLE V

OBLIGATIONS OF THE CONTROLLER AND PROCESSOR OF THE PERSONAL DATA DATABASES

Article 28.- Obligations

The controller and processor of the personal data databases, as applicable, have the following obligations:

28.1 Process the personal data only after obtaining the informed, express and unequivocal consent of the data subject, unless there is an authoritative law.

28.2 Not to compile personal data by fraudulent, unfair or illegal means.

28.3 Compile personal data that are updated, necessary, relevant and adequate in connection with the determined, explicit and legal purposes for which they were obtained.

28.4 Not to use the personal data processed for purposes other than those that motivated their compiling, except in case of anonymization or dissociation procedure.

28.5 Store the personal data in a manner that would make it possible for the data subject to exercise his rights.

28.6 Eliminate and replace or, if applicable, complete the personal data processed when it is aware of their inaccurate or incomplete character, without prejudice to the rights of the data subject in this regard.

[handwritten]

28.7 Eliminate the personal data processed when they are no longer necessary or relevant for the purpose for which they were compiled or when the term for processing has expired, unless there is an anonymization or dissociation process.

28.8 Provide to the National Authority for Personal Data Protection the information concerning the processing of personal data required by it and allow it access to the personal data databases administered by it for the performance of their functions.

28.9 Others established in this law and its regulation.

TITLE VI
PERSONAL DATA DATABASES

Article 29.- Creation, modification or cancellation of personal data databases

The creation, modification or cancellation of publicly and privately administered personal data databases will be subject to the provisions of the regulation, guaranteeing the publicity on their existence, purpose and identity and domicile of their controller and, if applicable, their processor.

Article 30.- Provision of personal data processing services

When personal data processing services are rendered on behalf of third parties, they may not be applied or used for a purpose other than that appearing in the contract or agreement executed, or be transferred to other persons, including for their storage.

After the performance of the service concerned by the contract or agreement, as the case may be, the processed personal data must be eliminated unless there is express authorization of the party on whose behalf such services are rendered when it is reasonably presumed that there is a possibility for additional tasks, in which case they may be kept in the due security conditions for up to the term established by the regulation of this Law.

Article 31.- Codes of conduct

The entities representing the controllers or processors of privately administered personal data databases may issue codes of conduct establishing rules for the processing of personal data intended to ensure and

improve the operating conditions of the information systems based on the guiding principles established in this Law.

TITLE VII

NATIONAL AUTHORITY FOR PERSONAL DATA PROTECTION

Article 32.- Competent entity and legal system

The Ministry of Justice, through the National Department of Justice, is the National Authority for Personal Data Protection. For the proper performance of its functions it may create offices in the entire country.

The National Authority for Personal Data Protection is governed by the provisions of this Law, its regulation and the pertinent articles of the Regulation for Organization and Functions of the Ministry of Justice.

The National Authority for Personal Data Protection may carry out all actions necessary to achieve the object and other provisions of this Law and this regulation. For this purpose it has sanctioning power pursuant to Law No. 27444, Law of General Administrative Procedure or its replacement as well as coactive power pursuant to Law No. 26979, Law of Procedure for Coactive Execution or its replacement.

The National Authority for Personal Data Protection must present periodically a report on its activities to the Ministry of Justice.

Article 33.- Functions

The National Authority for Personal Data Protection will carry out administrative, guiding, regulatory, decision making, supervisory and sanctioning functions listed below.

33.1 Represent the country to the international instances in matters of personal data protection.

33.2 Cooperate with foreign authorities for personal data protection in order to carry out their tasks and generate bilateral and multilateral cooperation mechanisms for mutual assistance and due mutual help when required.

33.3 Administer and keep updated the National Register of Personal Data Protection.

33.4 Publicize through the Institutional Portal the updated list of publicly and privately administered personal data databases.

33.5 Promote campaigns of spreading and promotion concerning personal data protection.

33.6 Promote and reinforce a culture of protection of the personal data of children and adolescents.

33.7 Coordinate the inclusion of information about the importance of private life and personal data protection in the curricula of the schools at all levels and also support the training of teachers in these topics.

33.8 Issue authorizations, when applicable, pursuant to the regulation of this Law.

33.9 Answer questions about personal data protection and the meaning of the current rules in the matter, especially those issued by it.

33.10 Issue a technical opinion concerning the bills referring in full or in part to personal data, which will be binding.

33.11 Issue the corresponding guidelines for the better application of the provisions of this Law and its regulation, especially in matters of security of personal data databases and supervise compliance therewith, in coordination with the sectors involved.

33.12 Promote the use of self regulation mechanisms as an additional instrument for personal data protection.

33.13 Execute inter-institutional and/or international cooperation agreements in order to assure the rights of the persons in matters of personal data protection processed in and out of the national territory.

33.14 Process requests for the private interest of the citizen or the general interest of the community, as well as requests for information.

33.15 Hear, investigate and resolve the complaints lodged by the data subjects for the violation of the rights granted to them and issue provisional and/or corrective measures, as established in the regulation.

33.16 Assure compliance with the laws related to personal data protection under respect of their guiding principles.

33.17 Obtain from the controllers of personal data databases the information it deems necessary for compliance with the rules on personal data protection and the performance of its functions.

33.18 Supervise the personal data processing carried out by the controller and processor of the personal data databases and, in case of illegality, order the appropriate actions, pursuant to the Law.

33.19 Start investigations, ex officio or by complaint of a party, for presumed acts contrary to the provisions of this Law and its regulation and apply the corresponding administrative sanctions, without prejudice to the provisional and/or corrective measures established by the regulation.

33.20 The other functions assigned to it by this Law and its regulation.

Article 34. National Register of Personal Data Protection

There is created the National Register of Personal Data Protection as an administrative register under the management of the National Authority for Personal Data Protection in order to record, in a differentiated manner, at national level, the following:

34.1 Publicly or privately administered personal data databases as well as the data concerning them necessary for the exercise of the rights of the data subjects, according to the provisions of this Law and the regulation.

34.2 The authorizations issued according to the regulation of this Law.

34.3 The sanctions, provisional and/or corrective measures imposed by the National Authority for Personal Data Protection according to this Law and its regulation.

34.4 The codes of conduct of the entities representing the privately administered personal data databases controllers or processors.

34.5 Other acts of registration according to the regulation.

Any person may consult in the National Authority for Personal Data Protection the existence of personal data databases, their purposes, as well as the identity and address of their controllers and, if applicable, their processors.

Article 35.- Confidentiality

The staff of the National Authority for Personal Data Protection are subject to the obligation to keep the confidentiality of the personal data learned by them in connection with their functions. This obligation will survive even after the termination of any relationship with said National Authority, under their liability.

Article 36.- Resources

The following are the resources of the National Authority for Personal Data Protection:

36.1 The fees for the right to process administrative procedures and services under its competence.

36.2 The amounts collected by it in fines.

36.3 The resources obtained from non-reimbursable international technical cooperation.

36.4 Bequests and donations received by it.

36.5 Resources transferred to it pursuant to the Law.

The resources of the National Authority for Personal Data Protection will be earmarked to finance the expenses necessary for the performance of its operations and for its functioning.

TITLE VIII
VIOLATIONS AND ADMINISTRATIVE SANCTIONS

Article 37.- Sanctioning procedure

The sanctioning procedure is initiated ex officio by the National Authority for Personal Data Protection or by complaint of a party in case of presumed commission

of acts contrary to the provisions of this Law or its regulation, without prejudice to the procedure followed under article 24 of this Law.

The Resolutions of the National Authority for Personal Data Protection exhaust the administrative channel.

The resolutions of the National Authority for Personal Data Protection may be challenged by administrative-litigation action.

Article 38.- Violations

Any action or omission in violation of the provisions of this Law or its regulation constitutes a sanctionable violation. Violations are qualified as mild, serious and very serious. The characterization of the violations, the levels of the amount of the fines and the procedure for their application will be set forth in the regulation of this Law.

Article 39.- Administrative sanctions

In case of violation of the rules of this Law or its regulation, the National Authority for Personal Data Protection may apply the following fines:

39.1 Mild violations will be sanctioned with a minimum fine of 0.5 (zero point five) Tax Units up to 5 (five) Tax Units.

39.2 Serious violations will be sanctioned with a fine of more than 5 (five) Tax Units up to 50 (fifty) Tax Units.

39.3 Very serious violations will be sanctioned with a fine of more than 50 (fifty) Tax Units up to 100 (one hundred) Tax Units.

The fine imposed may not exceed under any circumstances 10% (ten percent) of the annual gross income received by the presumed violator during the previous fiscal year.

The National Authority for Personal Data Protection will determine the violation committed and the amount of the fine that may be imposed by duly motivated Resolution. For the levels of the amount of the fines, the criteria established in article 230 section 3) of Law No. 27444, Law of General Administrative Procedure or its replacement will apply.

The fine will be imposed without prejudice to the disciplinary sanctions enforced on the staff of the public entities in the cases of publicly administered personal data databases as well as indemnity for damage and the applicable criminal sanctions.

Article 40.- Coercive fines

Pursuant to article 199 of Law No. 27444, Law of General Administrative Procedure, or its replacements, the National Authority for Personal Data Protection may impose coercive fines for an amount not exceeding ten (10) Tax Units, for violation of the obligations subject to sanction imposed in the sanctioning procedure. The coercive fines will impose after the end of the performance term.

The imposition of coercive fines does not prevent the exercise of other forced execution means pursuant to article 196 of Law No. 27444.

The regulation of the law will govern the aspects related to the application of coercive fines.

FINAL ADDITIONAL PROVISIONS

One.- Regulation

The regulation of this Law will be approved by Supreme Decree with the endorsement of the Minister of Justice.

For the preparation of the draft regulation, a Multisectoral Commission will be created, presided by the National Authority for Personal Data Protection. The draft regulation will be prepared within a maximum term of one hundred twenty (120) business days from the installation of the Multisectoral Commission which must occur within no more than 15 (fifteen) business days.

Two.- Security guideline

The National Authority for Personal Data Protection will prepare the security guideline of the information administered by personal data databases within no more than one hundred twenty (120) business days. Until the approval and enforcement of said guideline, the current sectoral provisions in the matter will be maintained.

Three.- Adjustment of management documents and of the Sole Text of Administrative Procedure of the Ministry of Justice

After the creation of the National Authority for Personal Data Protection within the maximum term of one hundred twenty (120) business days, the Ministry of Justice will prepare the relevant modification in its management documents and in its Sole Text of Administrative Procedure.

Four.- Adjustment and proposal for specific regulations on personal data

Within a term of no more than 60 (sixty) business days under the guidance and supervision of the National Authority for Personal Data Protection, the competent public entities will review the regulations on personal data and prepare the necessary proposals for their adjustment to the provisions of this Law. In case of absence of specific regulations and if it is indispensable they will make the appropriate proposals. As applicable, special data processing conditions will be kept in specific sectors.

Within thirty (30) business days after the issuance of the favorable technical opinion of the National Authority for Personal Data Protection, said entities must approve or, if applicable, support the approval of the corresponding regulatory proposals.

Five.- Preexisting personal data databases

The personal data databases created prior to this Law and its respective regulations must be adjusted to this law within the term established by the regulation. However, their controllers must declare them to the National Authority for Personal Data Protection according to the provisions of this Law.

Six.- Habeas Data

The rules established in the Constitutional Procedural Code on the processing of Habeas Data will apply at constitutional level, regardless of the administrative level concerned by this Law. The administrative procedure established in this Law does not constitute a prior channel for the exercise of the right through constitutional process.

[handwritten]

Seven.- Functions of the National Institute for the Defense of Competition and Protection of Intellectual Property - INDECOPI

In matters of violation of the rights of consumers in general through the services and information given by the Private Risk Information Centers - CEPIRS or similar, as part of consumer relations, the general rules on consumer protection apply, and the competent entity for the supervision of said compliance is the Commission for Consumer Protection of the National Institute for the Defense of Competition and Protection of Intellectual Property - INDECOPI, which must assure the permanent suitability of the services and the transparency of the information given to consumers, without prejudice to the function of the National Authority for Personal Data Protection to protect the rights of the data subjects concerning the information administered by the CEPIRS or similar.

Eight.- Sensitive information

For the purposes of Law No. 27489, Law which regulates private centers of risk information and data subject protection, sensitive information means the information defined as sensitive data by this Law.

Equally, it must be specified that the confidential information referred to in section 5), article 17 of the Sole Amended Text of Law No. 28706, Law of Transparency and Access to Public Information constitutes sensitive data pursuant to the scope of this Law.

Nine.- Lack of interference with the powers of the Tax Administration

The provisions of this law will not be interpreted to the detriment of the powers of the Tax Administration concerning the information found and required in its records, as well as the performance of its functions.

Ten.- Financing

The implementation of the actions necessary for the application of this Law is carried out with charge to the institutional budget of the Ministry of Justice and the resources referred to in article 36 of this law, without requiring additional resources from the Public Treasury.

Eleven.- Effective Date

This Law will enter in effect within thirty (30) business days from the publication of its regulation in the official gazette "El Peruano," except as provided in Title II in the first paragraph of article 32, and in the First, Second, Third, Fourth and Tenth Additional Final Provisions which will be in effect as of the day following the publication of this Law.

To be communicated to the President of the Republic for enactment.

[signature]
ALAN GARCÍA PÉREZ
Constitutional President of the Republic

[signature]
JAVIER VELÁZQUEZ QUESQUÉN
President of the Council of Ministers

[handwritten]