DEPARTMENT OF
TRADE & INDUSTRY
PHILIPPINES

Republic of the Philippines

Department of Trade and Industry

DEPARTMENT ADMINISTRATIVE ORDER NO. 08
Series of 2006

SUBJECT: Prescribing Guidelines for the Protection of Personal Data in Information and Communications System in the Private Sector

Section 1. **Declaration of Policy**

1.1 Whereas, the State recognizes the vital role of information and communications technology in nation building, as well as its own obligation to ensure network security, connectivity and neutrality of technology for the national benefit;

1.2 Whereas, under the E-Commerce Law (R.A. No. 8792), the Department of Trade and Industry (DTI) shall direct and supervise the promotion and development of electronic commerce in the Philippines with relevant government agencies, without prejudice to the provisions of Republic Act 7653 (Charter of Bangko Sentral ng Pilipinas) and Republic Act 8791 (General Banking Law of 2000);

1.3 Whereas, the issuance of clear, transparent, predictable and enforceable rules to clarify and ensure the protection of personal data in an information and communications system in the private sector will encourage and promote the development of Electronic Commerce in the Philippines, enhance its competitiveness in the new economy, protect the consumer, and encourage efficiency and transparency in commercial transactions;

1.4 Whereas the protection of users, in particular with regard to privacy, confidentiality, anonymity and content control shall be pursued through policies driven by choice, individual empowerment, and industry-led solutions. It shall be in accordance with applicable laws. Subject to such laws, business should make available to consumers and, where appropriate, business users, the means to exercise choice to privacy, confidentiality, content control and, under appropriate circumstances, anonymity;

1.5 Whereas, rules and guidelines for the Protection of Personal Data in Information and Communications System in the Private Sector that are technology neutral will help ensure continued private sector initiative and innovation, and encourage consumer trust;

1.6 And finally, recognizing that where appropriate, market-driven, contractual arrangements and codes of practice are better tools for protection of personal data in an information and communications system, developing user confidence in electronic commerce.

1.7 Now, therefore, the following guidelines for the protection of personal data in information and communications system in the private sector (hereinafter referred to as the "Guidelines") are hereby prescribed and promulgated for the compliance of all concerned.

Office of the Secretary
4/F, Industry & Investments Building, 385 Sen. Gil J. Puyat Avenue, 1200 Makati City, Philippines
Telephone: (632) 899-7450 • Fax: (632) 896-1166 E-mail:PBFavila@boi.gov.ph
www.dti.gov.ph

Section 2. **Objective and Sphere of Application**

2.1 These "Guidelines" are intended to encourage and provide support to private entities to adopt privacy policies for the protection of personal data in information and communications system in the private sector.

2.2 The "Guidelines" prescribe the rules governing data protection certifiers. As business organizations, data protection certifiers are encouraged to formulate, establish and implement unique types of certifications for each industry sector with the view to supporting and promoting various types of privacy programs.

2.3 The "Guidelines" likewise apply to the processing of all types of personal data whether such data refers to any natural or legal person, and without regard to whether or not that personal data is of local origin or from foreign countries.

Section 3. **Definition of Terms**

For the purposes of these "Guidelines", the following terms are defined, as follows:

3.1 *Accredit*ation – Third party attestation by the DTI Accreditation Office related to a conformity assessment body conveying formal demonstration of its competence to carry out specific conformity assessment tasks.

3.2 *Certification*- Third party attestation related to products, processes, systems, or persons. The grant thereof is on a company level basis or on a per activity or program basis.

3.3 *Consent of the data subject*- any freely-given, specific, and informed expression of will whereby data subjects agree to the processing of personal data relating to them.

3.4 *Data controller* - a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

3.5 *Data processor* (in relation to personal data) - any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

3.6 *Data Protection Certifier (or "Certifier")* - an independent third party duly accredited by the DTI Accreditation Office pursuant to these guidelines to certify the privacy program of a Licensee Company and thereafter, to monitor and oversee its implementation and enforcement. Certifiers must have:

3.6.1 Adequate knowledge and expertise concerning the handling and protection of personal information during the course of business activities, and, the ability to properly conduct business relating to setting privacy standards with such measures as certifying and checking web site privacy and email policies, scrutinizing online and offline privacy practices, and resolving consumer privacy problems.

3.7 *Data Subject* -the person to whom personal data relates.

3.8 *DTI Accreditation Office* – the body officially designated by the DTI Secretary to govern the implementation of these "Guidelines".

3.9 *Electronic document* – information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored, processed, retrieved or produced electronically.

3.10 *Information and Communications System* – a system for generating, sending, receiving, storing or otherwise processing electronic data messages or electronic documents and includes the computer system or other similar device by or in which data is recorded or stored and any procedures related to the recording or storage of electronic data message or electronic document.

3.11 *Licensee Company* - any data processor or data controller duly certified by the DTI-accredited Data Protection Certifier as having a Privacy Program compliant with, and meeting the minimum standards provided by these Guidelines.

3.12 *Person* – any natural or juridical person including, but not limited to, an individual, corporation, partnership, joint venture, unincorporated association, trust or other juridical entity, or any governmental authority.

3.13 *Personal Data* - any information relating to an identified or identifiable natural person.

3.14 *Privacy Program* - the policy, procedure, system, regulation, practice, or process maintained, adopted and used by a Licensee Company for the protection of personal data.

3.15 *Processing* – any operation or set of operations which is performed upon personal data, whether or not by automatic means.

Section 4. **General principles for the protection of personal data**

4.1 Personal data must be:

4.1.1 Collected for specified and legitimate purposes determined before collecting personal data and are later processed in a way compatible with those purposes;

4.1.2 Processed accurately, fairly and lawfully;

4.1.3 Accurate, and, where necessary for the processing of personal data, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing must be restricted.

4.1.4 Identical, adequate and not excessive in relation to the purposes for which they are collected and processed;

4.1.5 Kept in a form, which permits identification of data subjects for, no longer than is necessary for the purposes for which the data were collected and processed.

4.2 Criteria for lawful processing of personal data. - Personal data processing is permitted only if not prescribed otherwise by law, and at least one of the following conditions exists:

4.2.1 The data subject has given his or her unambiguous consent;

4.2.2 The personal data processing results from contractual obligations of the data subject;

4.2.3 The data processing is necessary to a data controller for the performance of his or her lawful obligations but in such cases, the processing shall be permitted only to fulfill the intention of the parties; or

4.2.4 The data processing is necessary to protect vitally important interests of the data subject, including life and health.

4.3 Disclosure of Personal Data to Data processor

4.3.1 A data controller may entrust personal data processing to a personal data processor provided a written contract is entered into between them;

4.3.2 A personal data processor may process personal data entrusted to him or her only within the scope determined in the contract and in accordance with the purposes provided for therein;

4.3.3 Prior to commencing personal data processing, a personal data processor shall perform safety measures determined by the data controller for the protection of the system in accordance with the requirements in this "Guidelines" and the E-Commerce Law.

4.4 Storage of data - Personal data may be stored and used only for as long as it is necessary to achieve the purpose for which it was processed. Unless otherwise stipulated in acts on individual types of personal data, personal data shall either be deleted from a personal data or blocked once the purpose from the preceding paragraph has been achieved.

4.5 Rights of the data subject- The data subject is entitled-

4.5.1 To be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller.

4.5.1.1 If that is the case, to be given by the data controller a description of:

4.5.1.1.1 The personal data of which that individual is the data subject,

4.5.1.1.2 The purposes for which they are being or are to be processed, and

4.5.1.1.3 The recipients or classes of recipients to whom they are or may be disclosed.

4.5.2 To be notified -

4.5.2.1 The information constituting any personal data of which that individual is the data subject, and

4.5.2.2 Any information available to the data controller as to the source of those data, and

4.5.2.3 Where the processing by automatic means of personal data of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performances at work, his creditworthiness, his reliability or his conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him, to be informed by the data controller of the logic involved in that decision-making.

4.6 Rights to information - A data subject also has the right to request the following information:

4.6.1 The designation, or name and surname, and address of the data controller;

4.6.2 The purpose, scope and method of the personal data processing;

4.6.3 The date when the personal data concerning the data subject was last rectified;

4.6.4 The source from which the personal data were obtained unless the disclosure of such information is prohibited by law; and

4.6.5 The processing methods utilized for the automated processing systems, concerning the application of which individual automated decisions are taken.

4.7 Data subject's right of access to his or her personal data. A data subject has the right, within a period of thirty (30) days from the date of submission of the relevant request, to receive from the data controller or data processor the information specified in the preceding Section in writing.

4.8 Data subject's right to request rectification, destruction of his personal data or restriction of further processing of his personal data.

4.8.1 A data subject has the right to request that his or her personal data be supplemented or rectified, as well as that their processing be suspended or that the data be destroyed if the personal data are incomplete, outdated, false, unlawfully obtained or are no longer necessary for the purposes for which they were collected. If the data subject is able to substantiate that the personal data included in the personal data processing system are incomplete, outdated, false, unlawfully obtained or no longer necessary for the purposes for which they were collected, the data controller has an obligation to rectify this inaccuracy or violation without delay and notify third parties who have previously received the processed data of such.

a) If information has been retracted, a data controller shall ensure the accessibility of both the new and the retracted information, and recipients thereof receive that the information mentioned simultaneously.

4.9 Right to object. - A data subject has the right to object (in writing, orally or in any other form) to the processing of his or her personal data if such will be used for commercial purposes.

Section 5. **Voluntary Accreditation**

A certification shall declare that the Privacy Policy employed by Licensee Company and examined by a Data Protection Certifier duly accredited by the Department of Trade and Industry (DTI) Accreditation Office, utilizes commercially appropriate and internationally recognized standards. The certification also covers the trustworthiness of the Data Protection Certifier's practices.

5.1 Responsibilities Arising from Accreditation

5.1.1 Pursuant to Department Administrative Order No. 01, series of 2005, prescribing the rules governing the voluntary accreditation of conformity assessment bodies, the DTI Accreditation Office shall accredit Data Protection Certifiers based on Philippine National or International Standards and/or guidelines.

5.1.1.1 Responsibilities of the DTI Accreditation Office

5.1.1.1.1 Receive and process applications for accreditation.

5.1.1.1.2 As necessary, organize teams to undertake assessment of applicants for accreditation.

5.1.1.1.3 Maintain and publish a registry of duly accredited bodies.

5.1.1.1.4 Issue certificate of accreditation to qualified applicant bodies based on established accreditation criteria.

5.1.1.1.5 Suspend or revoke accreditation of bodies that do not consistently comply with the terms and conditions of accreditation.

5.1.1.1.6 Establish and update criteria for accreditation of Data Protection Certifiers thru stakeholder consultations.

5.1.1.1.7 Receive and investigate the complaints against Licensee Companies and Data Protection Certifiers.

5.1.1.1.8 Maintain a list of all Philippine-DTI Accreditation Office Licensees of the accredited Data Protection Certifiers and publicly disclose this list.

5.1.1.1.9 Require certifiers to provide DTI Accreditation Office with additional information in the application, such as:

- Types and levels of data protection compliance certification
- Evaluation procedures of data processors
- List of all personnel certified to perform the necessary assessment to data processors.

5.1.1.2 Responsibilities of the Accredited Data Protection Certifier

5.1.1.2.1 In addition to the responsibilities as stated in DAO 1, Series of 2005 (certified copy attached hereto) under the terms and conditions of the certificate of accreditation, the Accredited Data Protection Certifier shall perform the following:

5.1.1.2.1.1 Report to DTI Accreditation Office the name of Licensee Company within 3 days upon issuance of data protection compliance certification.

5.2 Accreditation Criteria

5.2.1 The applicant must be a registered Philippine firm.

5.2.2 Shareholders and personnel of the registered Philippine firm have never been convicted of any violation under the E-Commerce Law.

5.2.3 The applicant must be recognized or licensed to provide data privacy or protection compliance certification by an international organization or firm.

5.3 Applications and Renewal for Accreditation

5.3.1. Accreditation under this Order is voluntary. Application shall be made in an official form which may be secured from the DTI Accreditation Office.

5.3.1.1. Every application to be an accredited Data Protection Certifier shall be made in such form and manner as the DTI Accreditation Office may, from time to time determine, and shall be supported by such information as the DTI Accreditation Office may require, such as, but not limited to, the following:

5.3.1.1.1. Types and levels of data protection compliance certification.

5.3.1.1.2. Evaluation procedures of data processors.

5.3.1.1.3. Resumes of all personnel certified to perform the necessary assessment to data processors.

5.3.2. The DTI Accreditation Office may require applications for renewal of accreditation in concurrence to the validity of the Data Protection Certifier's license to issue compliance certification to data processors.

5.3.3. A certificate of accreditation shall be subject to such conditions, restrictions, and limitations as the DTI Accreditation Office may, from time to time, determine.

5.4. Non-Renewal of the Accreditation of the Data Protection Certifier

5.4.1. If the Data Protection Certifier has no intention to renew its accreditation certificate, it shall –

5.4.1.1. Inform DTI Accreditation Office in writing not later than three (3) months before the expiry of the accreditation certificate;

5.4.1.2. Inform all its licensee companies in writing not later than six (6) months before the expiry of the accreditation certificate, and

5.4.1.3. Advertise such intention in a daily newspaper and in a manner, as the DTI Accreditation Office may determine, not later than two (2) months before the expiry of the accreditation certificate.

5.5. Grounds for Refusal to Grant or Renew the Accreditation of a Data Protection Certifier

5.5.1. DTI Accreditation Office shall refuse to grant or renew an accreditation certificate if:

5.5.1.1. The Data Protection Certifier or its substantial shareholder or any trusted person has been convicted, whether in the Philippines or elsewhere, of an offense which involved a finding that it or he acted fraudulently or dishonestly, or has been convicted of an offense under the E-Commerce Act or this Order;

5.5.1.2. There are other circumstances, such as complaints filed at the DTI Accreditation Office, which are likely to reflect the improper conduct of business by, or discredit on the method of conducting the business of, the applicant or its substantial shareholder or any of the trusted persons.

5.6 Revocation or Suspension of the Accreditation Certificate

5.6.1 The DTI Accreditation Office may suspend the accreditation certificate for a period of thirty (30) days on any of the following grounds:

5.6.1.1 If the Data Protection Certifier fails to carry on business for which it was accredited within three (3) months from issuance thereof;

5.6.1.2 If the DTI Accreditation Office, based on complaints or lawsuits filed, has evidence to prove that the Data Protection Certifier or its shareholder or personnel has not performed its duties efficiently, honestly or fairly;

5.6.1.3 If the Data Protection Certifier fails to correct the non-compliance within the suspension period of thirty (30) days, the accreditation certificate shall be revoked.

5.6.1.4 If the same non-compliance occurs for the second time, the accreditation certificate shall be revoked.

5.6.2 An accreditation certificate is revoked if the Data Protection Certifier is wound up.

5.6.3 The DTI Accreditation Office may also revoke the accreditation certificate of a Data Protection Certifier at the latter's express and specific request.

5.6.4 The DTI Accreditation Office shall not revoke or suspend the accreditation certificate on the grounds provided above without first giving the Data Protection Certifier an opportunity to explain and be heard.

5.7 Effect of Revocation or Suspension of the Accreditation Certificates

5.7.1 For the purposes of this Order, a Data Protection Certifier, whose accreditation is revoked or suspended, shall not be deemed accredited from the date that the DTI Accreditation Office revokes or suspends the certificate, as the case may be.

5.7.2 The revocation or suspension of an accreditation certificate of a Data Protection Certifier shall not affect:

5.7.2.1 Any agreement, transaction or arrangement entered into by the Data Protection Certifier, whether the agreement, transaction or arrangement was entered into before or after the revocation or suspension of the accreditation certificate, or

5.7.2.2 Any right, obligation or liability arising under any such agreement, transaction or arrangement.

5.8 Appeal against Refusal to issue the Certificate of Accreditation or Revocation/Suspension of the Certificate of Accreditation

Where -

5.8.1 the DTI Accreditation Office refuses to grant or renew an accreditation certificate under Section 5.5, or

5.8.2 the DTI Accreditation Office revokes or suspends accreditation certificate under Section 5.6, or

5.8.3 any person who feels aggrieved by the decision of the DTI Accreditation Office may, within fifteen (15) days from receipt of the written notice of the same, appeal to the ***Secretary of the DTI*** whose decision shall be final.

5.8.4 If an appeal is made against a decision made by the DTI Accreditation Office, the DTI Accreditation Office may, if appropriate, defer the execution of the decision, as the case may be, until a decision is made by the ***Secretary of the DTI*** or until the appeal is withdrawn.

5.8.5 In considering whether or not to defer the execution of the decision, the DTI Accreditation Office shall consider whether the deferment is prejudicial or not to the interests of any subscriber of the Data Protection Certifier or any other party who may be adversely affected.

5.8.6 When an appeal is made to the ***Secretary of DTI***, a copy of the appeal shall be provided to the DTI Accreditation Office.

5.8.7 Before filing the appeal, the appellant may file a motion for reconsideration with the DTI Accreditation Office within fifteen (15) days from receipt of the written notice of the refusal to grant or renew the certificate of accreditation, or of the revocation/suspension of the certificate of accreditation. The pendency of the said motion shall suspend the running of the 15-day period to appeal.

5.9 Change in Management or Personnel

5.9.1 An accredited Data Protection Certifier shall inform the DTI Accreditation Office of any changes in the appointment of any person as its director or chief executive, or of any person to perform functions equivalent to that of the chief executive, within 3 working days from the date of appointment of that person.

5.10 The following fees shall be collected from the applicants and DTI Accreditation Office accredited certifiers:

5.10.1 Application & Assessment Fee (Initial & Renewal)	P 15,000.00
Accreditation Fee (Payable upon issuance of Original or Renewal Certificate of Accreditation)	P 50,000.00

5.10 The DTI Accreditation Office shall not refund any fee paid if the application is not approved, withdrawn or discontinued or if the Certificate is suspended or revoked.

Section 6. **Lawful Access to Personal Data in an Information and Communications System**

Access to personal data in an information and communications system shall only be authorized in favor of the individual or entity having a legal right to the possession or the use of the file and solely for the authorized purposes. It shall not be made available to any person or party without the consent of the individual or entity in lawful possession, or in the absence of court order.

Section 7. **Obligation of Confidentiality**

Except for the purposes authorized under these "Guidelines", any person who obtained access to personal data in an information and communications system pursuant to any power conferred under the E-Commerce Law, shall not convey to or share the same with any other person.

Section 8. **Security of Data**

8.1 The data controller and data processor must implement appropriate organizational and technical measures intended for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure as well as against any other unlawful processing. These measures must ensure a level of security appropriate to the nature of the data to be protected and the risks represented by the processing and must be specified in a written document or its equivalent (data processing regulations approved by the data controller, a contract concluded by the data controller and the data processor etc.).

8.2 The data controller shall himself process personal data and/or shall authorize the data processor to do so. If the data controller authorizes the data processor to process personal data, he/she must choose a processor providing guarantees in respect of adequate technical and organizational data protection measures and ensuring compliance with those measures.

8.3 When authorizing the data processor to process personal data, the data controller shall stipulate that personal data must be processed only on instructions from the data controller.

8.4 The relations between the data controller and the data processor who is not the data controller shall be regulated by a written contract except where such relations are provided for by laws or other legal acts.

8.5 The employees of the data controller, the data processor and their representatives who are processing personal data must keep confidentiality of personal data if these personal data are not intended for public disclosure. This obligation shall continue even after their transfer to another position or upon termination of employment or contractual relations.

Section 9. **Privacy Complaints Mechanism**

9.1 The purpose of the section is to provide a one-stop shop for complainants, whether based here in the Philippines or situated abroad, to report complaints related to personal data privacy violations under these guidelines. The DTI Accreditation Office shall establish a Privacy Complaints Office and designate a Privacy Complaints officer. The Privacy Complaints Office shall act as a central repository of complaints related to any privacy violations committed by private entities under this "Guidelines".

9.2 Within three (3) days from receipt of any complaint, the DTI Accreditation Office shall forward the complaint to the relevant government agency/ies concerned. The DTI Accreditation Office Privacy Complaints Office shall also provide assistance to complainants to enable them to file their complaints before the proper venue.

Section 10. **Separability Clause**

In the event that any of the provision of this Order is declared invalid or unconstitutional, all the provisions not affected shall remain valid and in effect.

Section 11. **Effectivity**

This Order shall take effect after fifteen (15) days following the publication of its full text in one (1) newspaper of general circulation or in the Official Gazette. It shall also be published in the DTI website.

Makati City, July 21 2006.

Recommended by:

THOMAS G. AQUINO
Senior Undersecretary

Approved by:

PETER B. FAVILA
Secretary