

Notification of the Electronic Transactions Commission

Subject: Policy and Practice in protection of personal information of the State agency

B.E. 2553

Personal information which has been collected, archived, used or disseminated in data message format is a fundamental human right securing protection. At present, the information and communication system has been widely applied in conjunction with conducting electronic transactions. Also, in order to make electronic transactions of state agencies secure, reliable, and protective of personal information, the Electronic Transactions Commission deems appropriate to require that the policy and practice in protection of personal information of state agencies shall have the same standard.

By virtue of Sections 6, 7 and 8 of the Royal Decree Prescribing Rules and Procedures of Electronic Transactions in the Public Sectors of B.E. 2549, the Electronic Transactions Commission issues this Notification as a preliminary guideline for state agencies to use in setting the policy and practice in protection of personal information in electronic transactions, as follows:

Clause 1 State agency which collects, archives, uses, disseminates or does any other act in relation to the data of the subscriber of electronic transactions shall prepare a written policy in protection of personal information with the following minimum essential substances:

(1) Limited collection of personal information

Collection and archiving of personal information shall have a limited scope and use a legal and fair procedure, and the data owner shall be informed or grant consent, as the case may be.

(2) Quality of personal information

Personal information which has been collected and archived shall be in accordance with powers and duties and objectives for legal operations of the state agency.

(3) Determination of objectives in collection and archiving

Objectives of collection and archiving of personal information shall be recorded at the time of collection and archiving of personal information, including the use of such data afterwards. And if the objectives of collection and archiving are changed, an amendment record shall be made as evidence.

(4) Limitations in the application of personal information

Disclosure or display or appearance made in any other way of the personal information which is inconsistent with the objectives of the collection and archiving of data shall be prohibited unless the data owner provides consent or it is a case where the law prescribes as practicable.

(5) Security

Security measures of personal information shall be properly provided in order to prevent any wrongful loss, access, destruction, use, conversion, alteration or disclosure of the data.

(6) Disclosure about operations, practice and policy relating to personal information

Operations, practice and policy relating to personal information shall be disclosed, and a procedure that can examine the existence, features of such personal information, objectives of applying the data, controller and establishment of the personal information controller.

(7) Participation by the data owner

Personal information controller shall inform the data owner of the existence or details of such personal information upon request within a reasonable time period in accordance with a procedure in a format, including any expenses as appropriate (if any).

Controller of personal information shall be enjoined from refusing to provide an explanation or information to the data owner, successor, heir, legal representative or curator under the law.

Controller of information shall prepare a record of objections to archiving, correctness, or any other acts involving the data of the data owner as evidence.

(8) Responsibilities of the controller of information

Controller of personal information shall comply with the measures stated above in order to make operations pursuant to the policy regarding personal information protection in accordance with the standard of this Notification.

Clause 2 State agency shall prepare a practice in protection of personal information of the subscriber containing at least the following items:

(1) Basic data consists of:

(a) Name of the state agency to which the policy in protection of personal information belongs.

(b) Details of the enforcement scope of the personal information protection policy which the State agency collects, archives or uses in accordance with the objectives.

(c) Every change of the objective or policy in protection of personal information shall be notified to and ask for consent from the data owner first in accordance with the procedure and within the specified time in such notice, such as, 15-day prior notice notified to the data owner by sending via the electronic mail or publishing on the first page of the website, unless the law prescribes otherwise.

In obtaining the data owner's consent, clarity on which objective the state agency asks for such consent shall be made.

(2) Collection, categorisation and use of personal information

State agency conducting electronic transactions which collect data via the website or format of filling out paper data and then converting such data into the electronic system or archiving in other method, shall describe details of the data collection in a type and category, including data which will not be stored, and which objection the collected and archived data shall be used by a manner or with a procedure causing the data owner to be informed. Details of such collection and archiving of data shall be announced or notified to the data owner.

State agency providing services through a website shall exhibit details of the collection of data through the website of such agency, including usage of data which shall at least specify which part of the website or in which webpage the data is collected and archived, and shall provide clear details as to the procedure in collection

and archiving of such data, e.g. archiving with a requirement of registration or filling out a questionnaire etc.

State agency shall collect, archive and use personal information to prepare the following details:

(a) Communications between state agencies

State agency that will contact the subscriber through the electronic procedure shall give prior notice to the subscriber. The subscriber may inform his or her intention to be contacted through any other means.

(b) Use of Cookies

State agency shall specify on its website about use of cookies linked to the personal information that it will use the cookies for which objective and purpose and be entitled to deny a link to the cookies.

(c) Demographic Information

State agency shall have a website for collection of demographic information, such as, gender, age and occupation that can be linked to the identification data, that specifies the collection and archiving procedure of such data in the personal information protection policy, and that provide an explanation on the objective of such data usage, inclusive of granting other persons to share such data.

(d) Log Files

State agency arranging website services that automatically record the entry and exit, e.g., IP address, prior and later websites entered and exited and the category of browser program which can link such data with the identification data shall specify the collection and archiving procedure of such data in the personal information protection policy and provide an explanation on objectives of usage, inclusive of granting other persons to share such data.

(e) State agency shall specify the data archived through the website as the data that people have an option whether “to give or not to give” and such state agency shall provide another communication channel for the subscriber who does not wish to give data through the website.

(3) Display a link of providing personal information to other agency or organisation

Collection of data through the website of state agency that has a link providing the personal information to other state agency or organization shall be displayed by the state agency as to a name of the collector of information through the website, or name of the entitled person in the data subject collected and name of all entitled persons to access the said data, including the category of data which shall be shared with such agency or organization as well as the name of the person obligated to comply with the personal information protection policy for the subscriber's knowledge.

State agency shall inform the subscriber and obtain prior consent before changing the data link under the first paragraph with other agency or organisation.

(4) Collection of data from various sources

State agency that receives data from the website's subscriber and will integrate such data with such person's data acquired from another source shall specify in the personal information protection policy as to the purpose of such data collection, for instance, the website receives data about a name and e-mail address from the subscriber through the entry of data pursuant to the questionnaire via the website and will integrate such data with the data regarding the subscriber's biography received from another source.

(5) Authorizing another person to use or disclosing personal information

State agency shall also specify in the personal information protection policy that there is another person who will access or use the data collected by the agency through the website and that the authorized access, use or disclosure of such data is in line with the legal requirement of the state agency conducting as such.

(6) Collection, archiving, use and disclosure of the data about the subscriber

State agency collecting, archiving, using and disclosing the personal information which desires to proceed with another action other than the objective of collecting the personal as prescribed, e.g., unnecessary collection, archiving, usage and disclosure of personal information, or disclosure of personal information to another person, shall specify in the personal information protection policy as to the

right of the subscriber to choose whether to allow the state agency to collect, archive or not archive, use or not use, and disclose or not disclose such data.

The subscriber's exercise of the option under the first paragraph shall include granting the option in a form that the state agency must ask for explicit consent from the owner of such personal information first and granting the option in a form that awards a right to the subscriber to deny the use or disclosure of personal information for another objective other than the objectives of the personal information collection. The option shall be validly provided before the website will contact with the subscriber for the first time and, in case of an exercise of the option in the form prohibiting usage of the personal information different from the original objective, the agency owner of the website shall specify in the personal protection information to inform the subscriber of the procedure of sending the second contact of the website as well.

(7) Access, correction, and update

State agency shall specify a procedure by which the website's subscriber can access and rightly correct or update his or her personal information collected and archived by such state agency in the website.

(8) Security of personal information

State agency collecting personal information by means of providing the security procedure for the collected and archived personal information befitting maintenance of secrecy of the personal information in order to prevent wrongful alteration of such data, including prevention of any act resulting in the data not availability, shall take actions as follows:

(a) To promote consciousness to take responsibility about the security of personal information to the personnel, staff or employee of the agency through the regular dissemination of information, providing knowledge, organizing seminars and training with regard to such matter for personnel in the organisation.

(b) To prescribe clear rights and limitation of such rights in accessing the personal information of its personnel, staff or employee in each level of ranking, and provide a record, including the back-up data as to the access or entry for usage of

the personal information in an appropriate time period or under the legally prescribed time period.

(c) To audit and assessment of security risks of the entire website or information system at least once a year.

(d) To prescribe appropriate and specific measures for security of personal information with utmost importance or may affect the feelings, beliefs, public order and good morals who are subscribers of the state agency, or may clearly cause damage or impact to the rights and liberties of the data owner, e.g., debit or credit card numbers, identification numbers, personal identification numbers, nationality, religion, beliefs, political views, health, sexual behavior, etc.

(e) To provide careful measures in the security of the personal information belonging to a person not exceeding eighteen years of age by utilizing the specific and appropriate procedure.

(9) Website contact

Website providing information to the subscriber in communicating with the state agency shall provide either contacting information to the usual establishment or that through an online. The contacting information that the state agency should specify shall at least be comprised of the following data:

- (a) Name and address
- (b) Telephone number
- (c) Fax number
- (d) E-mail address

Clause 3 State agency shall prepare the policy and practice in protection of the personal information under the principles of clauses 1 and 2. For the state agency that receives a trust mark from another agency or organisation performing a duty to issue the trust mark, such state agency shall demonstrate the policy and practice in protection of the personal information certified by such agency or organisation issuing or certifying the trust mark to the Electronic Transactions Commission.

Trust mark pursuant to the first paragraph means a mark which certifies that such agency has a standard in protecting the public personal information in

Unofficial Translation

Volume 127 Special Part 126 Ngor Government Gazette

1 November 2010

conducting electronic transactions issued by the agency or organisation legally established to perform a duty in auditing and certifying the issuance of trust mark to applicants for certification.

Clause 4 State agency shall clearly designate a title of the personal information protection policy regarding and, in the case of policy improvement, specify the day, time and year on which improvement or change of such policy shall be made.

Clause 5 This Notification shall come into force on the day following its publication in the Government Gazette.

Notified on the 1st day of October B.E. 2553

Juti Krairiksh

Minister of information and Communication Technology

Chairman of Electronic Transactions Commission