Article Content

Title：	Enforcement Rules of the Personal Data Protection Act CH
Amended Date：	2016-03-02
Category：	National Development Council（國家發展委員會）

Article 1 The Enforcement Rules of the Personal Data Protection Act (these "Enforcement Rules") are enacted in accordance with Article 55 of the Personal Data Protection Act (the "PDPA").

Article 2 A "person" or "individual", as referred to under the PDPA, shall mean a living natural person.

Article 3 The circumstances where a data subject can be "indirectly identified", as referred to under Subparagraph 1, Paragraph 1, Article 2 of the PDPA, shall mean the circumstances where a government or non-government agency possessing such data cannot directly identify the data subject, unless it compares, combines or connects such data with other data.

Article 4 Personal data pertaining to a person's "medical records", as referred to under Subparagraph 1, Paragraph 1, Article 2 of the PDPA, shall mean the data specified in the subparagraphs of Paragraph 2, Article 67 of the Medical Care Act.
Personal data pertaining to a person's "healthcare", as referred to under Subparagraph 1, Paragraph 1, Article 2 of the PDPA, shall mean medical histories and any other data pertaining to checkups or treatments implemented by physicians or other medical professionals for the purpose of treating, correcting or preventing diseases, harms or disabilities of human body or for other legitimate medical reasons, or shall mean other data produced from the prescription, medication, operation or disposition based on the findings of the above-mentioned checkups.
Personal data pertaining to a person's "genetics", as referred to under Subparagraph 1, Paragraph 1, Article 2 of the PDPA, shall mean the information on a heredity unit, consisting of one segment of deoxyribonucleic acid (DNA) of human body, for controlling the specific functions thereof.
Personal data pertaining to a person's "sex life", as referred to under Subparagraph 1, Paragraph 1, Article 2 of the PDPA, shall mean the personal data on sexual orientation or sexual habits.
Personal data pertaining to a person's "physical examination",

as referred to under Subparagraph 1, Paragraph 1, Article 2 of the PDPA, shall mean the data produced by medical examinations conducted not for the purpose of diagnosing or treating a specific disease.
Personal data pertaining to a person's "criminal records", as referred to under Subparagraph 1, Paragraph 1, Article 2 of the PDPA, shall mean the records of deferred prosecutions, ex officio non-indictments, or a final guilty verdict rendered by a court and its enforcement.

Article 5 "Personal data file", as referred to under Subparagraph 2, Paragraph1, Article 2 of the PDPA, includes the backup file(s).

Article 6 "The act of deleting", as referred to under Subparagraph 4, Paragraph 1, Article 2 of the PDPA, shall mean to erase the personal data from the personal data file.
"Internal transfer", as referred to under Subparagraph 4, Paragraph 1, Article 2 of the PDPA, shall mean the data transfer within a government or non-government agency.

Article 7 The collection, processing or use of personal data by the commissioned legal person, group or natural person shall comply with the same laws and regulations applicable to the commissioning agency.

Article 8 When commissioning another to collect, process or use personal data, the commissioning agency shall properly supervise the commissioned agency.
The scope of supervision prescribed in the preceding paragraph shall include at least the followings:
1. the planned scope, category, specific purpose and time period of the collection, processing or use of personal data;
2. the measures taken by the commissioned agency in accordance with Paragraph 2 of Article 12;
3. the third party, if any, further commissioned by the commissioned agency;
4. the information that must be notified to the commissioning agency and the remedial measures that must be taken in the event that the commissioned agency or its employees violate(s) the PDPA or other laws and regulations relating to the protection of personal data;
5. any reserved matters for which the commissioned agency is required to obtain prior instructions from the commissioning agency; and
6. the return of any medium containing personal data and the deletion of any personal data stored and possessed by the commissioned agency due to its performance of the engagement contract between the commissioning agency and the commissioned

agency, upon the termination or cancellation thereof.
For the purpose of supervision prescribed under Paragraph 1, the commissioning agency shall carry out regular inspections to verify the commissioned agency's performance of the engagement contract and document the findings of such inspections.
The commissioned agency may collect, process or use personal data but only to the extent within the commissioning agency's instructions. If the commissioned agency considers that the commissioning agency's instructions are in contravention of the PDPA or other laws and regulations relating to the protection of personal data, the commissioned agency shall forthwith notify the commissioning agency.

Article 9 "Law", as referred to under Subparagraph 1 of the proviso to Paragraph 1 of Article 6, Subparagraph 1 of Paragraph 2 of Article 8, Subparagraph 1 of the proviso to Paragraph 1 of Article 16, Subparagraph 1 of Paragraph 1 of Article 19, and Subparagraph 1 of the proviso to Paragraph 1 of Article 20 of the PDPA, shall mean laws, or those regulations specifically and expressly authorized by laws.

Article 10 "Statutory duties", as referred to under Subparagraphs 2 and 5 of the proviso to Paragraph 1 of Article 6, Subparagraphs 2 and 3 of Paragraph 2 of Article 8, Subparagraph 2 of the proviso to Paragraph 1 of Article 10, Subparagraph 1 of Paragraph 1 of Article 15, and Article 16 of the PDPA, shall mean the official authority of government agencies prescribed in the following legal instruments:
1. laws, or those regulations authorized by laws;
2. self-governance ordinances;
3. those self-governance regulations authorized by laws or self-governance ordinances; or
4. those regulations authorized by laws or central government regulations to govern the commissioning matters.

Article 11 "Statutory obligations", as referred to under Subparagraphs 2 and 5 of the proviso to Paragraph 1 of Article 6, and Subparagraph 2 of Paragraph 2 of Article 8 of the PDPA, shall mean the obligations of non-government agencies prescribed by laws or those regulations specifically and expressly authorized by laws.

Article 12 "Proper security and maintenance measures", as referred to under Subparagraphs 2 and 5 of the proviso to Paragraph 1 of Article 6, "security and maintenance measures", as referred to under Article 18, and "proper security measures", as referred to under Subparagraph 2 of Paragraph 1 of Article 19 and Paragraph 1 of Article 27 of the PDPA, shall mean the technical or

organizational measures taken by a government agency or non-government agency for the purpose of preventing personal data from being stolen, altered, damaged, destroyed or disclosed.
The measures prescribed in the preceding paragraph may include the following and shall be proportionate to the intended purposes of personal data protection:
1. allocating management personnel and reasonable resources;
2. defining the scope of personal data;
3. establishing a mechanism of risk assessment and management of personal data;
4. establishing a mechanism of preventing, giving notice of, and responding to a data breach;
5. establishing an internal control procedure for the collection, processing, and use of personal data;
6. managing data security and personnel;
7. promoting awareness, education and training;
8. managing facility security;
9. establishing an audit mechanism of data security;
10. keeping records, log files and relevant evidence; and
11. implementing integrated and persistent improvements on the security and maintenance of personal data.

Article 13 "The personal data that has been disclosed to the public by the data subject", as referred to under Subparagraph 3 of the proviso to Paragraph 1 of Article 6, Subparagraph 2 of Paragraph 2 of Article 9, and Subparagraph 3 of Paragraph 1 of Article 19 of the PDPA, shall mean the personal data voluntarily disclosed by the data subject to non-specific persons or a large number of specific persons.
"The personal data that has been made public lawfully", as referred to under Subparagraph 3 of the proviso to Paragraph 1 of Article 6, Subparagraph 2 of Paragraph 2 of Article 9, and Subparagraph 3 of Paragraph 1 of Article 19 of the PDPA, shall mean personal data that has been published, publicly announced or disclosed to the public through other lawful means in accordance with laws or those regulations specifically and expressly authorized by laws.

Article 14 In accordance with the Electronic Signatures Act, a data subject's "consent in writing", as referred to under Subparagraph 6 of the proviso to Paragraph 1 of Article 6, Paragraph 2 and 3 of the proviso to Article 11 of the PDPA, may be given in an electronic form.

Article 15 If "a separate declaration of agreement", as referred to under Paragraph 2, Article 7 of the PDPA, is to be provided concurrently with other expressions of intent in the same document, the data collector shall, where appropriate on the

document, make the data subject aware of the details of such agreement and confirm his/her consent.

Article 16 The obligation to inform data subjects as required under Articles 8, 9, and 54 of the PDPA may be fulfilled via verbal words, in writing, over the phone, via text messages, email, fax, electronic documents or other means that can effectively make the information known or available to the data subjects.

Article 17 The "data that may not lead to the identification of a specific data subject", as referred to under Subparagraph 4 of the proviso to Paragraph 1 of Article 6, Subparagraph 4 of Paragraph 2 of Article 9, Subparagraph 5 of the proviso to Paragraph 1 of Article 16, Subparagraph 4 of Paragraph 1 of Article 19, and Subparagraph 5 of the proviso to Paragraph 1 of Article 20 of the PDPA, shall mean the personal data replaced with codes, deleted data subject’s name, partially concealed, or processed via other means to the extent that the data subject may not be directly identified.

Article 18 The circumstances "where the material interests of any third parties may be adversely affected", as referred to under the Subparagraph 3 of the proviso to Paragraph 1 of Article 10 of the PDPA, shall mean the circumstances where any third parties' life, body, freedom, properties or other material interests may be harmed.

Article 19 When a data subject requests a government or non-government agency to correct or supplement his/her personal data in accordance with Paragraph 1, Article 11 of the PDPA, the data subject shall provide the agency with an adequate explanation therefor.

Article 20 The circumstances "where the specific purpose no longer exists" referred to under Paragraph 3, Article 11 of the PDPA shall mean any of the following circumstances:
1. the government agency has been dissolved or reorganized without another agency to take over its tasks;
2. the non-government agency has ceased its business or been dissolved without another agency to take over its business, or the non-government agency has changed the scope of its business, thereby causing the purpose for which the personal data were collected to be no longer applicable;
3. the specific purpose has been reached, and there is therefore no longer necessary to continue the processing and use of personal data; or
4. other circumstances where the specific purpose evidently can no longer be reached or no longer exists.

Article 21 The "necessity for the performance of an official or business duty", as referred to in the proviso to Paragraph 3, Article 11 of the PDPA, shall mean any of the following circumstances:
1. where a retention period is prescribed by laws or regulations, or agreed upon under a contract;
2. where there are sufficient reasons to believe that the deletion of the personal data will infringe upon the data subject's interests that warrant protection; or
3. where there are other legitimate reasons for not erasing the personal data.

Article 22 A notification given via "appropriate means", as referred to under Article 12 of the PDPA, shall mean a notification that is given in a prompt manner via verbal words, in writing, over the phone, via text messages, email, fax, electronic documents or other means that can effectively make the information known or available to the data subjects. However, if such notification entails disproportionate costs, a government or non-government agency may, taking into consideration the technical feasibility and privacy protection of the data subjects, notify the data subjects through the Internet, the media or other proper and public means.
A notification given under Article 12 of the PDPA shall include the facts pertaining to the data breach and the response measures already adopted to address such breach of personal data.

Article 23 A government agency shall make public of information under Article 17 of the PDPA within one month after the establishment of the personal data files; the same also applies to any modification thereof. The methods of making information public shall be specified and shall not be changed at random.
"Other appropriate means", as referred to under Article 17 of the PDPA, shall mean making public such information via government gazettes, newspapers, magazines, online newspapers or other means that allows the general public to make inquiries of such information.

Article 24 A government agency in possession of personal data files shall set forth security and maintenance rules for personal data.

Article 25 "Dedicated personnel", as referred to under Article 18 of the PDPA, shall mean personnel with the ability to manage and maintain personal data files and to adequately perform the regular task of securing and maintaining personal data and the files thereof for the agency.
To equip the dedicated personnel with the ability to secure and maintain personal data, the government agency shall hold

relevant professional training sessions or ensure that the dedicated personnel undergo such professional training.

Article 26 A "contractual or quasi-contractual relationship", as referred to under Subparagraph 2, Paragraph 1, Article 19 of the PDPA, is not limited to the relationship formed after the amendment to the PDPA has taken into effect.

Article 27 A "contractual relationship", as referred to under Subparagraph 2, Paragraph 1, Article 19 of the PDPA, shall include the contractual relationship between a non-government agency and a data subject, and also the relationship where a non-government agency and a data subject are either contacting, negotiating or communicating with, receiving delivery from or making delivery to a necessary third party for the purpose of performing the contract between the non-government agency and the data subject.
A "quasi-contractual relationship", as referred to under Subparagraph 2, Paragraph 1, Article 19 of the PDPA, shall mean any of the following:
1. any relationships involving the contact and negotiation between a non-government agency and a data subject before the execution of a contract for the purpose of preparing for or negotiating the terms of such contract or transaction; or
2. any relationships involving the communication between a non-government agency and a data subject upon the extinguishment of a contract due to the invalidation, rescission, cancellation or termination thereof or upon the complete performance of a contract, for the purpose of exercising their rights, performing their obligations, or ensuring the integrity of the personal data.

Article 28 "Publicly available sources", as referred to under Subparagraph 7, Paragraph 1, Article 19 of the PDPA, shall mean mass media, the Internet, news, magazines, government gazettes and other channels through which the general public may become aware of or come in contact with and then subsequently obtain personal data.

Article 29 When conducting the inspections in accordance with Article 22 of the PDPA, the inspectors shall fulfill their confidentiality obligations and uphold the reputation of those being inspected.

Article 30 When retaining or duplicating the personal data or the files thereof that may be confiscated or admitted as evidence in accordance with Paragraph 2, Article 22 of the PDPA, a receipt specifying the name, quantity, the owner, the location and time of retaining or duplicating of such data or files shall be issued.
After an inspection has been conducted in accordance with

Paragraphs 1 and 2, Article 22 of the PDPA, a record thereof shall be made.
If the record mentioned in the preceding paragraph is made onsite, such record shall be reviewed and signed by the inspected agency. A copy of the record shall be promptly given to the inspected agency. If the inspected agency refuses to sign the record, the reason thereof shall be specified on such record.
If the record is made off site afterwards, such record shall be delivered to the inspected agency, which shall be informed that it may submit relevant statements within a certain period of time.

Article 31 "Public interest groups", as referred to under Paragraph 1, Article 52 of the PDPA, shall mean incorporated charities, incorporated foundations or administrative entities established in accordance with the Civil Code or other laws and having the professional ability regarding the protection of personal data.

Article 32 The collected or processed personal data provided by a data subject before the effective date of the amended PDPA can continue to be processed and used within the scope of the specific purpose of collection. The use for another purpose shall comply with the provisions under the amended PDPA.

Article 33 The effective date of these Enforcement Rules shall be promulgated by the Ministry of Justice.