

University of New South Wales
University of New South Wales Faculty of Law Research Series
2011

Year 2011

Paper 58

Taiwan Revises Its Data Protection Act

Graham Greenleaf*

*University of New South Wales, g.greenleaf@unsw.edu.au

This working paper is hosted by The Berkeley Electronic Press (bepress) and may not be commercially reproduced without the permission of the copyright holder.

<http://law.bepress.com/unswwps-flrps11/art58>

Copyright ©2011 by the author.

Taiwan Revises Its Data Protection Act

Graham Greenleaf

Abstract

Taiwan's Computer Processed Personal Data Protection Act of 1995 was pioneering data protection legislation in Asia, but had many inherent defects. It had limited coverage, dealing generally with the public sector but only eight specified private sector areas. There was no single oversight body, enforcement being left to the Ministries responsible for each industry sector. Evidence of the enforcement or effectiveness of the Act is lacking, but commentators were of the opinion that the Act is ineffective.

The new Personal Data Protection Act enacted 26 May 2010 is in effect a new piece of legislation. It will not be brought into force until 2012 when the Enforcement Rules necessary for operation of some sections, are expected to be prescribed by the Executive Yuan. The Act is comprehensive in relation to both public and private sectors, and thus much more extensive than the previous Act in relation to the private sector. The revised Act still has no single oversight body, and does not create a data protection authority. Enforcement is left to the Ministries responsible for each industry sector. The obligations imposed by the Act have been considerably expanded, particularly those in relation to notice, and to sensitive data. Data exports ('international transmission') by private organisations ('non-public agencies') may be restricted by 'the central competent authority for the relevant industry' (A 21), but this is not an automatic prohibition on exports. The Act has the first example of an enforceable requirement to notify data subjects (but not the relevant authority) of data breaches enacted in Asian data protection legislation, although the data breach notification provisions in the 2011 Korean legislation is the first to come into force. However, the Taiwanese provision does not apply to all 'data breaches', only to those where the company or government agency has breached a provision of the Act. Contraventions of the Act, where damage is caused to another person, can be punished by imprisonment up to two years or

substantial fines. Potentially more important are the extensive provisions for damages actions, and for class action litigation (where ‘the rights of multiple subjects are injured by the same causal facts’) by representative organisations which have objectives of protecting personal data. While not as innovative as Korea’s new law, this Act does bring Taiwan up to many aspects of international standards.

Taiwan revises its Data Protection Act

Graham Greenleaf

Professor of Law & Information Systems, University of New South Wales

Published in two parts in *Privacy Laws & Business International Report*, Issues 108 (2010) and 109 (2011)

Part I: Improvements in Principles

Published as Greenleaf, G 'Taiwan revises its Data Protection Act: Improvements in Principles' 108 *Privacy Laws & Business International Newsletter* 8-10, December 2010

Taiwan's *Computer Processed Personal Data Protection Act* of 1995 was pioneering data protection legislation in Asia, but had many inherent defects (including limited coverage, both in terms of types of data and industry sectors, lack of notice requirements, limited rights of data subject, and limited penalties), and there was little evidence that it was enforced or observed (see D Tang 'Taiwan proposes amendments to its 1995 Data Protection Act' *PLBI Newsletter* February 2009, 19-20).

The new *Personal Data Protection Act* enacted 26 May 2010 is in effect a new piece of legislation. It will not be brought into force (on a date prescribed by the Executive: A 56) until late 2011 or early 2012 when the Enforcement Rules (A 55) necessary for operation of some sections, are expected to be prescribed by the Ministry of Justice. However, the Act provides ample detail of how different the new regime for data protection will be from the 1995 regime. This article analyses the obligations of data processors under the new Act, noting both innovative aspects, and a number of continuing deficiencies. A following article will analyse the rights of data subjects, and enforcement.

Scope and definitions

The definition of 'personal data' lists numerous categories, and also includes 'other data that could directly or indirectly identify that person', which seems to give it considerable breadth. 'Personal data file' means 'a set of personal data that is systematically built and can be searched or arranged' by automated or non-automated means. Other terms are defined by reference to one or other of these concepts, so the distinction is significant.

The Act distinguishes between a 'public agency' ('a central or local government agency or administrative juristic person that exercises public authority pursuant to law' and a 'non-public agency' ('a natural person, juristic person, or group other than those mentioned' in the definition of public agency), which we could equally call a 'private agency'. There are some distinctions between the obligations between the two types of agencies, but otherwise the Act is comprehensive in its scope.

Agents and sub-processors are covered by the provision deeming 'anyone retained to collect, process, or use personal data ... as one and the same as the retaining agency' (A 4).

There are only two general exemptions from the Act, but (as is normal) there are more specific exceptions from specific principles. 'Collection, processing, or use of personal

data by a natural person for purely personal or family activity purposes' (A 51.1) is an internationally standard exemption. However, an exemption for 'collection, processing, or use in a public place or public activity of audiovisual data that is not combined with any other personal data' (A 51.2) is a confusingly worded exemption that may cover the operation of CCTV, and photography/video in public places or of (undefined) 'public activity'.

This extra-territorial effect of the Act is extensive, but only in respect to Taiwanese nationals: it 'also applies to collection, processing, or use outside of the territory of the Republic of China by a public agency or non-public agency of personal data of nationals of the Republic of China' (A 51). We must assume that this only applies to agencies that have otherwise become subject to the Act, because otherwise it could apply to any company anywhere that ever processes data about a Taiwanese national, which could not be intended.

Key definitions – 'collection', 'processing' and 'use'

The obligations depend on which of three related terms are used to specify them. 'Collection' means 'obtaining personal data by any means' (A 2.3), an unusually broad definition encompassing collection by observation and extraction from books or databases, from third parties, and from unsolicited or transactional information. 'Processing' means 'the recording, input, storage, editing, correction, reproduction, searching, deletion, output, linking, or internal transfer of data for purposes of building or using a personal data file' (A 2.4). 'Processing' is therefore very broad but does not include collection, and it also does not explicitly include internal decision-making or actions based on use of personal data, nor the external disclosure of personal data (in contrast with 'internal transfer'. 'Use' means 'any utilization of collected personal data other than processing' (A 2.5). 'Utilization' would seem to encompass what in other jurisdictions is referred to as both 'internal use' and 'external disclosure'. 'Processing' therefore does not include 'use', and 'use' does not include 'processing' – and 'collection' is separate from either. Harm to data subjects will most often arise from 'use' of their personal data, so it may be expected that more strict obligations will apply to 'use'.

'Use' also does not seem to be limited to personal data in personal data files (in contrast to 'processing') but can it seems apply to personal data not held in such files, though it is not certain that this is what is intended. The expression 'collect, process, or use' is therefore the most comprehensive description of what can or cannot be done with personal data, and it or variants are used in various places in the Act where comprehensiveness is desired (Articles 3,4,5,6,11,21 and 51).

General obligations of public and private agencies

All types of agencies are subject to the general obligations in Articles 5-14 (including the data subject rights in Articles 10-14 discussed in the second part of this article), but there are also obligations specific to public agencies in Articles 15-18 (Chapter II) and to private agencies in Articles 19-27 (Chapter III).

Article 5 states the most general obligation as: 'Collection, processing, or use of personal data shall respect the rights and interests of the subject, shall be done in an honest and good-faith manner, may not exceed the scope necessary for the specific purposes, and shall have a legitimate and reasonable relation to the purposes of collection.' The requirements of good faith, necessity (relative to purpose), and 'reasonable' relation to

purpose of collection therefore suffuse everything that can be done with personal data. Any requirement for consent to processing must come from elsewhere in the Act.

Notification requirements

Whenever personal data is collected 'from a subject' (solicited or unsolicited) the collector must 'explicitly notify' the subject of the collector's name, purpose of collection, classification of data collected (this determines the relevant industry sector), 'period(s), region(s), counterparty(ies), and method(s) of use of the personal data', 'rights exercisable by the subject ... and method of exercise', and the effect on the subject's rights of not providing the data (A 8). A key question here is now precisely subjects will be advised of the 'method of exercise' of their rights, particularly to whom they should make complaints in a system where there is no central data protection authority. This is a potential area of weakness.

There are, however, overly-broad exemptions from this notification obligation. There are 5 justifiable exemptions: where another law exempts from the obligation to notify, where collection is necessary for the performance of a statutory duty or obligation, where notification 'would impair the exercise of statutory duties by a public agency' and (perhaps) 'would impair a material interest of a third party', and where the subject is fully aware of the contents of the notification. But exemption from notification merely because collection is necessary for the performance of a statutory duty or obligation effectively eliminates notification from a vast range of transactions and observations without a requirement of justification.

Where personal data is collected other than from the subject, the notice required by Article 8 must be given before processing or use of the data (or concurrently, in communications with the subject) (A 9). Additional exceptions are provided, including that the personal data has voluntarily been made public by the subject or otherwise has already lawfully been made public', or impossibility of notifying the subject (or their legal guardian), or statistical or research uses with anonymised results, or collection for 'public interest news broadcasting purposes'. The situations exempted from notification in A 8-II (discussed in the previous paragraph) are also exempted. Given the breadth of types of collection covered, broad exemptions from notice are needed.

In relation to previously collected personal data, notification is required to be completed within one year from the date the Act comes into force. Any processing or use of the data after that without such notification will violate Article 9 (A 54).

Public agency obligations

Less strict obligations are imposed on public agencies concerning their collection or processing of personal data (A 15), with stricter obligations imposed on its use (A 16).

Public agencies are required to have 'specific purposes' for *collecting or processing* personal data (A 15), and the processing would therefore have to 'have a legitimate and reasonable relation to the purpose of the collection' (A 5). In addition, public agencies may also only collect or process personal data in accordance with the scope necessary for the exercise of their statutory duties, or with the subject's written consent, or where 'there is no injury to the rights and interests of the subject' (A15). This last exemption might seem unduly broad and subjective, undermining the first two exceptions, but it must be borne in mind that a 'reasonable relation to the purpose of the collection' is still

required. While there is no requirement of consent for processing, it is only one grounds of justification, nevertheless, any processing does require one of these three justifications. This implies that processing injurious to the data subject is illegal unless necessary for a statutory duty (or with consent).

Public agencies may only *use* personal data in accordance with the scope necessary for the exercise of their statutory duties and 'in conformity with the specific purposes of collection' (not merely having a 'reasonable relation' to it). There follows a lengthy list of allowed uses of personal data allowed by public agencies not in conformity with the specific purpose of collection (A 16), including exceptions for uses based on express legal provisions, national security and other public interests, avoiding danger or harm to the interests of others, the subject's interests (avoiding danger to the subject's life, body, or property and benefiting the rights and interest of the subject), and written consent of the subject. Article 16 therefore covers two different kinds of uses: uses in conformity with the specific purpose of collection; and uses outside the specific purpose of collection (secondary uses). Article 15 only deals with collection and processing (and not use) and imposes different standards.

Public agencies must also comply with an 'openness' provision (A 17) requiring public disclosure on a website of the types of personal data files they keep.

Private sector obligations

As with public agencies, there are different obligations on the private sector for use of personal data than there are for its collection and processing. Private agencies can only *collect and process* personal data with the written consent of the subject, or under one of six other conditions: express legal provisions; contractual or quasi-contractual relationships; data already voluntarily or lawfully made public; certain anonymous research uses; a broad 'related to public interests' ground; or if 'obtained from a generally available source' (A19).

This last ground will not apply if the subject has 'has a material interest in the prohibition of processing or use of the data that obviously is more deserving of protection'. If a collector or processor knows that this exception applies, they must on their own initiative delete or cease processing of the data. They must also do so on request.

Use of personal data (either internal or by disclosure) by private agencies has similar allowed secondary uses as use by public agencies (A 20). Additionally, there are special provisions for direct marketing uses, allowing consumer opt-out, and requiring the provision of a method of opting out at the 'initial time' marketing is done.

Of greatest importance, however, is the Article 20 exception for uses outside the purpose of collection 'to promote public interests'. When coupled with the exception for collection and processing 'related to public interest' (A 19), these provisions are interpreted as a broad 'media exemption'.

Sensitive data

The default position applicable to both public and private sector is that 'Personal data related to medical treatment, genetics, sexual life, health examinations, and criminal record may not be collected, processed, or used' (A 6). There is no definition in the Act

of any of these terms. Four exceptions are then made where expressly provided by law, where necessary for performance of statutory duties or obligations, where the personal data has voluntarily or lawfully been made public, and for certain research purposes (for which Regulations are to be made).

None of the specific provisions allowing collection, processing or use by either public agencies or private agencies, discussed above, apply to data covered by Article 6. Where an exception to Article 6 applies, it seems that the applicable provisions would then be the general provisions (Articles 5-9 and the subject rights).

Implications for companies involved in Taiwan

The obligations imposed by the Act have been considerably expanded, particularly those in relation to notice, and to sensitive data. Overseas companies involved in any sector of the Taiwanese economy will now have to pay more attention to data protection issues, due to the much broader scope of the legislation in the private sector. The extra-territorial scope of the Act, and its potential application to data exports, must also be considered. As will be explained in the concluding article, the data breach notification requirements (the first in Asia) will require companies subject to the Taiwanese law to adjust to a new obligation of uncertain scope. Increased penalties and exposure to actions for damages will also add considerable risk to the implications of these expanded principles.

Part II: Data breach notification and diffused enforcement

Published as Greenleaf, G 'Breach notification and diffused enforcement in Taiwan's DP Act' Privacy Laws & Business International Report, Issue 109, 12-13, February, 2011

This article commences by considering three further obligations of data users in Taiwan's revised *Data Protection Act*: considerably strengthened data export restrictions; ill-defined data security obligations; and the first data breach notification requirement in Asian legislation (for the other obligations of data users, see (2010) 108 PLBIR 8). The rights of data subjects, and the enforcement of both user obligations and data subject rights, are then discussed.

Data export restrictions

Data exports ('international transmission') by private organisations ('non-public agencies') *may* be restricted by 'the central competent authority for the relevant industry' (A 21), but this is not an automatic prohibition on exports. The authority may restrict exports which 'involve a material national interest' or are subject to treaty provisions. More significantly, it may do so if 'the receiving nation lacks sound laws and regulations to adequately protect personal data, such that the rights and interests of subjects are likely to be injured', or if an export is 'by a circuitous means to evade' such a prohibition. The use of the undefined term 'adequately' does of course suggest that a standard consistent with the EU data protection Directive is intended. But the key factor is that this is an export prohibition at the discretion of Taiwanese government agencies, and is definitely at the very weak end of the spectrum of export restriction laws.

'International transmissions' are defined to mean 'transnational (cross-border) processing or utilization of personal data' (A2.6), so it would seem that data that remains in Taiwan but is processed or used in any way from outside Taiwan is covered. However, 'collection' is not included, so if a Taiwanese person's data is collected from them by an entity outside Taiwan (such as over the Internet), this might not be covered by Article 21.

Confusing security obligations

Public agencies are only required to 'designate dedicated personnel' to handle security matters (A 18), but there is no stated standard of security of personal data that they are required to achieve. In contrast, private sector organisations are required to 'adopt appropriate security measures', and regulations detailing such security standards (and requiring adoption of security plans) can be made by the 'central competent authorities' for each industry sector (A 27). There is therefore a danger of a proliferation of different standards.

However, Article 5 requires of both the public and private sectors that 'collection, processing or use of personal data 'shall respect the rights and interests of the subject', so a general obligation to take reasonable security precautions may be implied from this.

Limited data breach notification

If a public or private sector agency 'violates any provision' of the Act, 'such that personal data is stolen, disclosed, altered, or otherwise impaired', then 'the agency, after investigating, shall notify the subjects by an appropriate means' (A 12).

This is a particularly important provision, the first example of an enforceable data breach notification in Asian data protection legislation. However, it has significant limitations. The obligation does not apply to all 'data breaches', only to those where the agency has breached a provision of the Act. So, theft of data by a third party where it could not be held that the agency was in breach of its security or other obligations, will not be covered. However, the notification requirement could apply not only where an agency failed to discharge its security obligations, but also where it breached some other provision of the Act, such as by disclosing personal data to third parties where it should not have done so, or where it made inappropriate use of data. Since failure to notify where appropriate under A 12 is itself a breach of the Act, damages could potentially result from over-defensive failure to notify.

The scope of Article 12 will remain unclear unless the Enforcement Rules clarify what is meant by 'an appropriate means', and to what extent agencies can delay notification by claiming they are still 'investigating'. Such devices could render the provision worthless. It is also impaired by lack of an obligation to inform the relevant supervisory authority.

Data subject rights

Access rights are subject to exceptions where national interests, or the execution of statutory duties, would be impaired (A 10). There is also what seems an over-broad exception where access 'would impair a material interest of the collecting agency or a third party', with no requirement that this be balanced against the importance of access

to the data subject. Public agencies are given an explicit discretion whether to charge fees (A 14).

All data users have a positive duty to 'maintain the accuracy' of personal data, and to correct or supplement them on their own initiative (A 11). Data subjects also have the right to request corrections or supplementation. Where data users have failed to correct or supplement personal data, they must inform prior recipients of that data after it has been corrected or supplemented.

Article 11 also requires data users to cease the processing or use of personal data in a number of circumstances: (a) where the accuracy of data is disputed, unless the processing or use is necessary for duties or business and the dispute is specifically noted; (b) wherever there is collection, processing or use in violation of the Act; and (c) where the purpose of collection has ceased to apply. These are positive obligations of data users, and may also be requested by data subjects. Data subjects do not, however, have the right to require cessation of processing of their data at any other times.

These data subject rights 'may not be waived in advance nor limited by special agreement' (A 3). Overall, this is a strong package of data subject rights.

Enforcement, offences and administrative fines

The revised Act still has no single oversight body, and does not create a data protection authority. Enforcement is left to the Ministries responsible for each industry sector. The details will not be known until the Enforcement Rules are made, but it seems that the Ministry of Justice will be responsible for the implementation of the Act by public agencies, and the Department of Commerce, Ministry of Economic Affairs, will have a lead role in the private sector. There are as yet no obvious transparency mechanisms to reveal how the Act will operate: no obligations to report complaints and their resolution, deliver annual reports and so on. Without them, it could be as opaque as the Japanese legislation.

Chapter V of the Act has extensive provisions for offences (requiring court prosecutions) and 'administrative fines' against private sector agencies, which can be imposed by the central competent authority for a particular industry.

Breaches of the Act, where damage is caused to another person, can be punished by imprisonment up to two years or fines of NT\$200,000 (about US\$6,700). Where there is intent to profit, this can increase to 5 years or NT\$1 million (A 41). This also applies to unlawful impairment of accuracy of a personal data file, with intent to gain a benefit (A 42). These offences can be committed by a Republic of China national from outside Taiwan (A 43). Where committed by a civil servant, the penalties are increased by 50% (A 43).

Private sector agencies can alternatively be subjected to an administrative fine by the central competent authority for a particular industry. For breaches of more important provisions, fines can be between NT\$50,000 and NT\$500,000 (about US\$15,000), and for other provisions between NT\$20,000 and NT\$200,000 (A 47 – A 49). Where such an administrative fine is imposed on an organisation, someone who represents the organisation is also to be fined a similar amount unless they can prove they fulfilled their duty to prevent such a breach (A 50).

Damages and class actions

Potentially more important are the extensive provisions in Chapter IV of the Act for damages actions, and for class action litigation. Public agencies have strict liability for 'injuring the rights of a subject' through breaches of the Act, with exceptions for damage due to 'natural disaster, accident, or other force majeure' (A 28). Private sector agencies, in contrast, are liable unless they can prove that they did not breach the provisions of the Act 'wilfully or negligently' (A 29).

For claims against any type of agency, injuries other than to property, including to reputation, may be claimed. If claimants cannot prove actual damage, they may ask the court to assess damages between NT\$500 and NT\$20,000 (US\$670). Where multiple persons are injured from the same event (such as a mass data spill) the aggregate damages are capped at NT\$200 million (about US\$6.7 million) unless greater damage is proved. There is a limitation period for commencement of actions of two years from when both damage and defendant are known, or five years from when the damage occurs (A 30). Claims are also governed by the State Compensation Act (against public agencies) and the Civil Code (against private sector agencies). There are complex provisions concerning which district court has jurisdiction (A 33).

The provisions for class action litigation (A 32, A 34 – A 40) require that 'the rights of multiple subjects are injured by the same causal facts'. An incorporated foundation or incorporated public interest association (these representative bodies are defined in A 32) can commence an action once it has received written consent from at least 20 injured subjects. There are procedures for such actions to be publicised and other potential claimants invited to join the action.

The representative bodies have to comply with strict requirements: (i) a foundation with assets of NT\$10 million, or an association with at least 100 members; (ii) articles including protection of personal data; and (iii) incorporation for at least three years.

The representative body must disburse damages received to those who authorised it to litigate, after deduction of litigation expenses (but with no remuneration) (A 39), and must act through a lawyer (A 40).

Implications for businesses dealing with Taiwan

Evidence of the enforcement or effectiveness of the previous version of the Act was lacking, and commentators were of the opinion that the Act was ineffective: 'insufficient and flawed' (Peng, 2003); 'many defects' (Tang, 2009); and 'full of loopholes' (Chuang, 2003). Criticisms included because of vague provisions, limited scope, and lack of any general supervisory agency. There was no known enforcement of the very limited existing provisions for data transfer restrictions.

The revised Act promises much stronger data protection, and requires more vigilance by foreign companies involved in transactions either with Taiwanese corporate partners or with Taiwanese consumers. But much will depend on whether the Enforcement Rules and their implementation make the legislation credible.

References

The author acknowledges the considerable assistance of Paul Cox and Shan Lee of Winkler Partners, Taiwan, in relation to translation of terms in the new legislation, and the valuable comments of Professor Dennis TC Tang of Academia Sinica.

Chuang, Tyng-Ruey (2003), "Personal data protection in Taiwan: Whose business?" *National Policy Quarterly*, volume 2, number 1, Pages 53-70; in Chinese with English abstract, at <http://www.iis.sinica.edu.tw/~trc/public/publications/npq03/>

Peng, Shin-yi (2003) 'Privacy and the construction of legal meaning in Taiwan' *The International Lawyer* Vol 37 No 4, 2003

Tang (2009) 'Taiwan proposes amendments to its 1995 Data Protection Act' PLBI Newsletter February 2009, 19-20

