



Introduction to Taiwan's Personal Data Protection PDPA

1. Taiwan Practice Group Introduction

In February 2023, Atsumi & Sakai established a Taiwan Practice Group (the "PG"). The PG plans to regularly publish a newsletter featuring information that we believe will be useful for inbound and outbound matters between Taiwan and Japan. The first issue already was published in English and Chinese (traditional) for overseas readers in February.

This newsletter discusses Taiwan's Personal Data Protection Act. Knowledge about the Personal Data Protection Act is essential for companies doing business in Taiwan.

Atsumi & Sakai includes a Taiwanese lawyer¹ among its associates, and our Fukuoka affiliated firm, A&S Fukuoka LPC, also has a Taiwanese lawyer² on staff.

2. Taiwan's Personal Data Protection Act

In Taiwan, as in Japan, the handling of personal data³ by companies is governed by the Taiwan's Personal Data Protection Act⁴ (hereinafter simply referred to as the "PDPA"). The PDPA was enacted to avoid infringement of personal rights and to promote the reasonable use of personal data.

3. Definition of Personal Data

(1) Personal Data

Under the PDPA, personal data means a natural person's name, date of birth, ID card number, passport number, features, fingerprints, marital status, family information, education background, occupation, medical records, genetic data, data concerning a person's sex life, records of physical examination, criminal records, contact information, financial condition, data concerning a person's social activities, and any other information that may be used to directly or indirectly identify such natural person (Article 2, Item (1) of the PDPA).

Although there are no clear rules in Taiwan regarding whether cookies, website browsing records, etc. constitute personal data, according to the definition of personal data above, it is possible that they do.

(2) Sensitive Personal Data

Certain personal data, including medical records, medical care, genetic, sexual life, physical examinations or criminal records, are treated as sensitive personal data and must be handled more carefully than other personal data (Article 6, Paragraph 1 of the PDPA).

¹ Not registered as a Foreign Lawyer in Japan.

² Not registered as a Foreign Lawyer in Japan.

³ In Taiwan, different from Japan, there is no differentiation between the concept of "Personal information" and "Personal Data." The official English translation of the PDPA mentions only "Personal Data."

⁴ The English version is published at <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=10050021>

4. Methods of Handling Personal Data

Under the PDPA, there are three methods for handling personal data; namely, collection, processing or use (Article 2, Item (3) - (5) of the PDPA).

- The term "collection" means the acquisition of personal data by any method.
- "Processing" means recording, entering, storing, editing, correcting, copying, retrieving, deleting, outputting, linking or internally transmitting information for the purpose of creating or using a personal data file.
- "Use" means any use other than processing.

5. General Principles for Handling Personal Data

● Collection and Processing

When collecting personal data, the parties whose data is to be collected must be clearly notified of the purpose of the collection and their rights, etc. regarding their personal data (Article 8, Paragraph 1 and Article 3 of the PDPA).

In order to collect and process personal data, there must be a valid reason for the data collection and such collection must fall under certain circumstances (e.g., there must be clear legal provisions that require such collection, there must be a contractual or contract-like relationship between the parties, with appropriate security measures in place, or the consent of the party whose information is to be collected must be obtained) (Article 19, Paragraph 1, Item (1) - (8) of the PDPA).

● Use

In principle, collected personal data may be used only to the extent necessary for the purpose for which it was collected. For example, if personal data is collected for the purpose of providing services, it is understood that, in principle, such personal data cannot be used for advertising and marketing purposes (Article 20, Paragraph 1 of the PDPA).

6. Use of Personal Data for Other Purposes

If collected personal data is used for purposes other than those for which it was collected, such use must comply with the explicit provisions of the law or requirements such as obtaining consent of the party whose data is collected (Article 20, Paragraph 1 of the PDPA). Consent in this case refers to an independent manifestation of intention by the parties concerned after the collector has explicitly notified them of the purpose and scope of use and the impact of consent on their rights and interests, but the form of consent is not restricted (Article 7, Paragraph 2 of the PDPA).

7. International Transfers (cross-border transfers)

When transferring personal data internationally, the competent authorities⁵ may restrict such international transfer if (Article 21 of the PDPA):

- (1) major national interests are involved;
- (2) special provisions in international treaties or agreements require such limitation;
- (3) the recipient country does not have complete laws and regulations regarding the protection of personal data and there is a risk of damaging the rights and interests of the parties concerned; or
- (4) such transfer avoids the PDPA by transferring personal data to a third country (or region) in a circumventive manner

Currently, the competent authorities are restricting the transfer of personal data to China for some industries.

⁵ There is now no centralized authority, instead, the monitoring of each industry is handled by the authority of each industry. It is reported that in 2024 the "Personal Data Protection Commission" will be established.

8. Data Portability Right

The so-called Data Portability Right⁶, as stipulated in the GDPR, is not stipulated in the PDPA.

9. Anonymized Information

Although the PDPA does not provide detailed provisions for anonymisation of personal data, personal data becomes "unidentifiable to a specific party" if it is coded, anonymized, partially hidden, or otherwise rendered unidentifiable (Article 17 of the Enforcement Rules of the PDPA).

If the manner in which the provider processed the information or the collector disclosed the information renders the information "unidentifiable to a particular party," then the information may be treated as follows:

- Sensitive personal data, which in principle is not permitted to be handled, may be collected, processed, and used by government agencies and academic research institutions when necessary for statistical or academic research for the purpose of medical care, hygiene, or crime prevention (Article 6, Paragraph 1, Item (4) of the PDPA).
- The obligation to notify the parties when collecting indirectly can be exempted when the information is necessary in the public interest for statistical or academic research purposes⁷(Article 9, Paragraph 2, Item(4) of the PDPA).
- Academic and research institutions may collect and process personal data when necessary in the public interest for statistical or academic research purposes (Article 19, Paragraph 1, Item (4) of the PDPA).
- If necessary in the public interest for the purpose of statistics or academic research by a government agency or academic research organization, companies may use the information for purposes other than the purpose for which it was collected (Article 20, Paragraph 1, Item (5) of the PDPA).

10. Engagement of Data Service Providers

A legal entity, organization, or individual engaged with the collection, processing, or use of personal data is considered the same as the consignor to the extent applicable by the PDPA. In other words, the consignee must comply with the regulations applicable to the consignor. In addition, the consignor must appropriately supervise the consignee (Article 4 of the PDPA, and Articles 7 and 8 of the Enforcement Rules of the PDPA).

11. Related Liability

● Civil Liability

Companies are liable to compensate for damages if they unlawfully collect, process, or use personal data in violation of the PDPA, or if they violate the rights of a party whose data is disclosed. However, this is not applicable if it can be proven that there was no willful intention or negligence (Article 29, Paragraph 1 of the PDPA).

● Criminal Liability

If a person, with the intention of obtaining unlawful gains for himself/herself or a third party, or with the intention of impairing another person's interests, violates the regulations on the collection, processing, or use of personal data, or breaches an order or decisions of international transfer by the competent authorities, which is sufficient to cause damage to others, the violating party shall be punished with imprisonment not exceeding five years and/or a fine not exceeding NT\$1,000,000 (Article 41 of the PDPA).

⁶ <https://gdpr-info.eu/art-20-gdpr/>

⁷ Essentially, if personal data that is not provided by the data subject is collected, the source of the personal data and related rights must be notified to the party whose data was collected before the processing and use of such personal data (Article 9 of the PDPA).

If a person, with the intention of obtaining unlawful gains for himself/herself or a third party, or with the intention of impairing another person's interests, unlawfully alters, deletes, or uses other unlawful methods to damage the accuracy of a personal data file (i.e., the collection of personal data that is created by a system and can be retrieved and organized by automated machines or other non-automated means (Article 2, Item (2) of the PDPA)), which is sufficient to cause damage to others, the violating party shall be punished by imprisonment for a term not exceeding five years or detention and/or a fine not exceeding NT\$1,000,000 (Article 42 of the PDPA).

● Administrative Liability

If a person unlawfully collects sensitive personal data, violates regulations on the collection, processing, or use of personal data, or breaches orders or decisions on international transfers by the competent authorities, a fine of NT\$50,000 to NT\$500,000 will be imposed and the violating party will be ordered to rectify the situation within a certain period of time. Failure to rectify the violation within the proscribed time period will result in punishment according to the number of violations (Article 47 of the PDPA).

If a company violates its obligation to notify when it collects personal data, etc., the competent authorities will set a period of time and order the company to rectify the situation. If the violation is not corrected within the proscribed time period, a fine of NT\$20,000 to 200,000 will be imposed, depending on the number of violations (Article 48, Paragraph 1 of the PDPA).

If a company fails to take appropriate security measures to prevent personal data from being stolen, tampered with, damaged, destroyed, or leaked, the competent authorities shall impose a fine of NT\$20,000 to NT\$2,000,000, and order the company to rectify the violation within a specified period of time. If the company fails to rectify the violation in time, a fine of NT\$150,000 to NT\$15,000,000 shall be imposed for each occurrence of the violation. Further, if it is a serious violation, an immediate fine of NT\$150,000 to NT\$15,000,000 may be imposed (Article 48, Paragraph 2 and 3 of the PDPA).

If a company is subject to a fine under the PDPA, its representatives and others will be subject to the same fine unless they can prove that they have fulfilled their duty of prevention (Article 50 of the PDPA).

12. Other relevant matters

At the time of writing this newsletter, in addition to the PDPA, the competent authorities may have established regulations for certain industries regarding the security management of personal data files, etc., and may stipulate work processes, supervision processes or reporting obligations, etc. Therefore, when handling personal data, companies should also be aware of relevant regulations other than the PDPA.

In addition, Taiwan has seen a number of personal data leakage incidents in recent years, and discussions regarding personal data protection laws have intensified. As a result, the PDPA was amended in May 2023, and other than a partial increase in the fines for administrative liability, a body with overall jurisdiction over the PDPA called the "Personal Data Protection Commission" will be established in the future (Article 1-1 of the PDPA), so please be aware of the effective date of related laws.

Since this is an area where legal changes occur frequently, it is advisable to seek professional advice.

End.

For more information on the Taiwan Practice Group, consisting of attorneys from Atsumi & Sakai and A&S Fukuoka LPC, please visit our website here.

<https://www.aplawjapan.com/global-coverage/taiwan>

THIS NEWSLETTER IS PROVIDED FOR INFORMATION PURPOSES ONLY; IT DOES NOT CONSTITUTE AND SHOULD NOT BE RELIED UPON AS LEGAL ADVICE.

Authors/Contacts

Yasuhiro Usui

Partner
A&S Fukuoka LPC*, Fukuoka Bar Association
E: yasuihiro.usui@aplaw.jp

Tomoyuki Kiyuna

Associate
A&S Fukuoka LPC*, Fukuoka Bar Association
E: tomoyuki.kiyuna@aplaw.jp

Marina Fu**

Associate
A&S Fukuoka LPC*, Taipei Bar Association
E: marina.fu@aplaw.jp

*Although A&S Fukuoka LPC is affiliated with Atsumi & Sakai Legal Professional Corporation, it is a separate corporation and is not a branch office of Atsumi & Sakai Legal Professional Corporation.
**Not registered as a Foreign Lawyer in Japan

Inquiries:

Atsumi & Sakai Taiwan Team
Email: jpg_taiwan@aplaw.jp

If you would like to sign up for A&S Newsletters, please fill out the [sign-up form](#).
Back issues of our newsletters are available [here](#).

Atsumi & Sakai is a multi-award-winning, independent Tokyo law firm with a dynamic and innovative approach to legal practice; it has been responsible for a number of ground-breaking financial deal structures and was the first Japanese law firm to create a foreign law joint venture and to admit foreign lawyers as full partners. Expanding from its highly regarded finance practice, the Firm now acts for a wide range of international and domestic companies, banks, financial institutions and other businesses, offering a comprehensive range of legal expertise.

Atsumi & Sakai has an outward-looking approach to its international practice, and has several foreign lawyers with extensive experience from leading international law firms, providing its clients with the benefit of both Japanese law expertise and real international experience.

We are the only independent Japanese law firm with affiliated offices located in New York, London and Frankfurt which, together with our Tokyo office and Fukuoka affiliated office, enables us to provide real-time advice on Japanese law to our clients globally.

Atsumi & Sakai

www.aplawjapan.com/en/

Tokyo Office: Fukoku Seimei Bldg., 2-2-2 Uchisaiwaicho, Chiyoda-ku, Tokyo 100-0011, Japan

Fukuoka Affiliate Office: Tenjin Bldg. 10F, 2-12-1 Tenjin, Chuo-ku, Fukuoka-shi, Fukuoka 810-0001 Japan

New York Affiliate Office: 1120 Avenue of the Americas, 4th Floor, New York, New York 10036

London Office: 4th Floor, 50 Mark Lane, London EC3R 7QR, United Kingdom

Frankfurt Affiliate Office: OpernTurm (13F) Bockenheimer Landstraße 2-4, 60306 Frankfurt am Main, Germany

NOTICES

1. ABOUT ATSUMI & SAKAI

Atsumi & Sakai is a partnership consisting of Atsumi & Sakai Legal Professional Corporation, a Japanese professional corporation, a foreign law joint venture under the Act on Special Measures Concerning the Handling of Legal Services by Foreign Lawyers with certain Registered Foreign Lawyers of our firm, a Japanese Civil Code partnership among Japanese lawyers, represented by Yutaka Sakai, a lawyer admitted in Japan, and a foreign law joint venture with Janssen Foreign Law Office, represented by Markus Janssen, a foreign lawyer registered in Japan to advise on the laws of the Federal Republic of Germany. In addition to lawyers admitted in Japan, our firm includes foreign lawyers registered in Japan to advise on the laws of the US States of New York and California, India, England and Wales, and the State of Queensland, Australia. Foreign lawyers registered in Japan to advise on state laws also are qualified to provide advice in Japan on the federal laws of their respective jurisdictions.

Atsumi & Sakai has established an office in London operating as Atsumi & Sakai Europe Limited (a company incorporated in England and Wales (No: 09389892); sole director Naoki Kanehisa, a lawyer admitted in Japan), and has established an affiliate office in New York operating as Atsumi & Sakai New York LLP (a limited liability partnership established in New York; managing partner Bonnie L. Dixon, a lawyer admitted in New York and a Registered Foreign Lawyer in Japan). We also have a partnership with A&S Fukuoka LPC in Japan (partner: Yasuhiro Usui, a lawyer admitted in Japan) and an affiliate office in Frankfurt operating as Atsumi & Sakai Europa GmbH - Rechtsanwälte und Steuerberater, a corporation registered in Germany providing legal and tax advisory services (local managing directors: Frank Becker, a lawyer, and Miyuki Hanaoka a tax advisor, both admitted in the Federal Republic of Germany).

2. LEGAL ADVICE

Japanese legal advice provided by Atsumi & Sakai and our global offices is provided by lawyers admitted in Japan. Advice provided in Tokyo in respect of any foreign law on which one of our foreign lawyers is registered in Japan to advise, may be provided by such a Registered Foreign Lawyer. None of Atsumi & Sakai Legal Professional Corporation, Atsumi & Sakai Europe Limited or Mr. Naoki Kanehisa is regulated by the Solicitors Regulation Authority for England and Wales, and none will undertake any reserved legal activity as defined in the United Kingdom Legal Services Act 2007. Advice provided in Germany on the laws of Germany will be provided by a lawyer admitted in Germany, and advice provided in New York on the laws of New York will be provided by a lawyer admitted in New York.