

Regional Data Privacy Frameworks “Understanding and Harmonizing Data Privacy Regulations”

Yvonne Lin
Formosan Brothers _ Taiwan
2024/03/02



Director/Managing Partner

Yvonne Y.F. Lin

University of Washington (Seattle,
U.S.A.), LL.M.

National Taipei (Chung Hsing)
University (Taiwan), LL.B.

Taiwan attorney-at-law
Taiwan Patent Attorney
Arbitrator in Taiwan

yvonne@mail.fblaw.com.tw

Experiences

- Director, Asian Patent Attorneys Association (APAA)
- Director, Taiwan Trademark Association (TTA)
- Co-chairperson of the Copyright Committee of APAA
- Committee member, Patent Examination Quality Consultation Committee of the Intellectual Property Office of the Ministry of Economic Affairs
- Chairperson, the International Affairs Committee of the Taiwan Patent Attorneys Association
- Vice Chairperson, the Intellectual Property Committee, Taiwan Bar Association
- Arbitrator, Chinese Arbitration Association, Taipei
- Asia Business Law Journal –Taiwan’s Top 100 Lawyers
- Legal Media 360 Ranked lawyers in Intellectual property
- Asialaw – Distinguished Practitioner

Practices

- Intellectual property
- Antitrust / Competition
- Data protection
- Biotechnology / Pharmaceuticals
- Corporate governance / legal compliance
- Merger and acquisition
- Emerging technologies
- Litigation and Arbitration

Content

Current Issues on Data Privacy Matters



Importance of Establishment of Regional Data Privacy Frameworks



Forecast on the future of Data Privacy





Current issues on Data Privacy matters

Dutch Data Protection Authority(DPA) fines Uber €10 million over privacy regulations infringement Jan 31, 2024

- Uber makes it difficult for drivers to access their personal information.
- Uber did not specify how long it retains the drivers' personal data.
- **Uber failed to address data transmission outside Europe:** Uber did not specify in their privacy terms and conditions...which specific security measures it takes **when sending this information to entities in countries outside the European Union.**



Sources: Dutch DPA <https://www.autoriteitpersoonsgegevens.nl/en/current/uber-fined-eu10-million-for-infringement-of-privacy-regulations/>

ChatGPT: Italy (the Garante) says OpenAI's chatbot breaches data protection rules

Jan 29, 2024

Italy's data protection authority "Garante" suspected ChatGPT breaches European Union (EU) privacy rules so banned its service last year and request OpenAI to take improvement measure.

In Jan. 2024, Garante said based on the outcome of the Italian DPA fact-finding activity, it concluded that the available evidence **pointed to the existence of breaches of the provisions contained in the EU GDPR.**



Sources: Garante per la protezione dei dati personali <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9978020>

Line operator (LY) reports around 440,000 items of personal data leaked

Nov 27, 2023

- As many as 440,000 items of personal data, including more than 300,000 linked to the Line messaging app, have been leaked.
- The leaked data included users' age groups, genders, and some of their service use histories, as well as information regarding the company's business partners and employees, such as email addresses, names and affiliations.
- The leakage was caused when malware infected a computer owned by an employee of a subcontractor used by the company's South Korea-based affiliate.
- Line has reported the case to the communications ministry →LINE Taiwan has also reported the case to the Taiwan authority "ADI". ADI requested Line Taiwan to submit solution for damages incurred by Taiwan users therefor.



Foxsemicon hit by ransomware Jan 17, 2024

- The website of Hon Hai Technology Group's affiliate Foxsemicon Integrated Technology Inc appeared to have been hijacked by a ransomware group "LockBit", displaying a message threatening to release the personal information of the company's customers and employee.
- Foxsemicon operates sites in the USA and China, with customers distributed across Europe and the USA. **The compromised personal data therefore presents a cross-border issue rather than a purely domestic one.**

>>>>> Your data is stolen and encrypted.

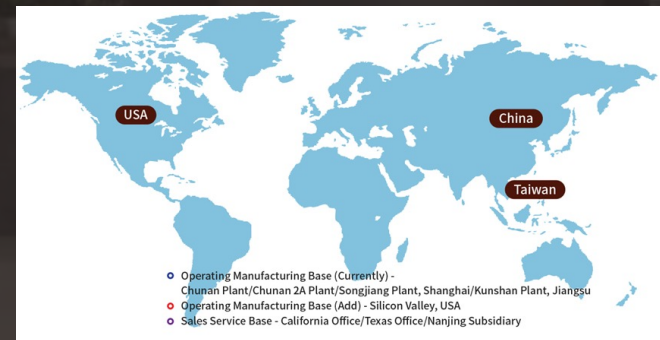
[\[List stolen and encrypted files\]](#)

TOTAL DATA VOLUME: 5TB

If you don't pay the ransom, the data will be published on our TOR darknet site.
Keep in mind that once your data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.

Customer information:
If you are a Foxsemicon customer, we have all your personal data. All your personal data will be freely available on the internet if Foxsemicon not pays money.

Information for employees:
If your management does not contact us, you will lose your job, as we are able to completely destroy Foxsemicon with no possibility of recovery, all media (BBC, The New York Times, The Wall Street Journal, The Washington Post) will inform you that the company no longer exists.



Sources: TAIPEI TIMES <https://www.taipeitimes.com/News/biz/archives/2024/01/17/2003812190>

“LockBit”, the world’s most prolific ransomware group, has been operating since 2019, it was targeting thousands of victims around the world with ransomware attacks that have cost billions of dollars in terms of both ransom payments and recovery costs

An international law enforcement task force called “Operation Cronos” which is law-enforcement agencies from 10 countries.



On 19 February, “Operation Cronos” posted a message on the site that read: “This site is now under the control of the National Crime Agency (NCA) of the UK, working in close cooperation with the FBI and the international law enforcement task force, ‘Operation Cronos’”

Sources: <https://www.weforum.org/agenda/2024/02/lockbit-ransomware-operation-cronos-cybercrime/>

Other issues of data privacy matter



Data privacy policies and measures in response to the rise of AI



Privacy risks from facial recognition and surveillance



Privacy risks from COVID-19 contact tracking technology



Cross-border matters



Importance of establishment of regional data privacy frameworks

A local data privacy incident can have global implications



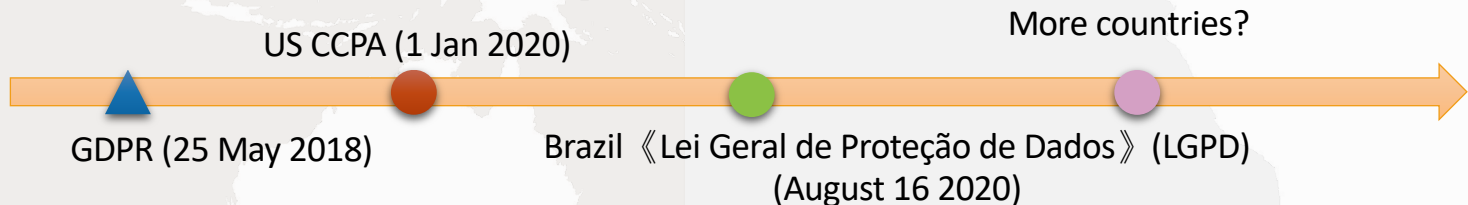
Take GDPR as an example...



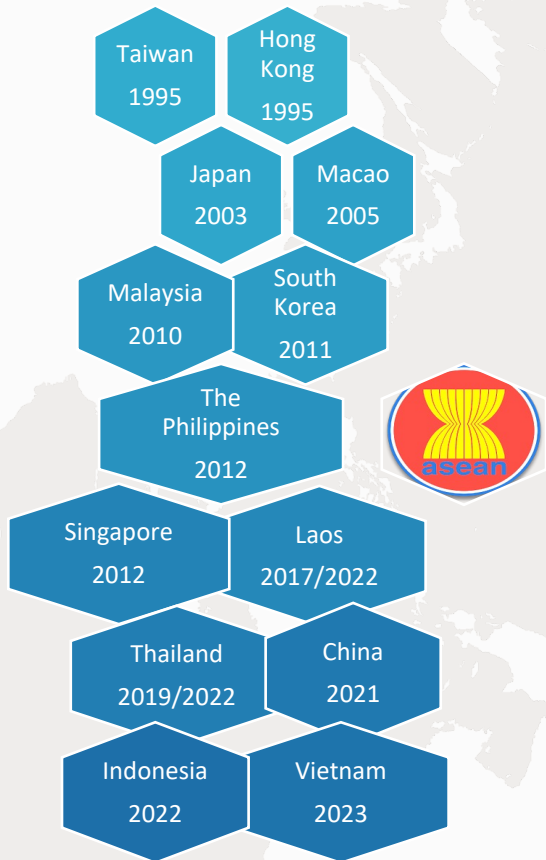
Long arm protection (Art. 3 GDPR Territorial scope)

- This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller **or processor not established in the Union**, where the processing activities are related to:
 - (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
 - (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
- This Regulation applies to **the processing of personal data by a controller not established in the Union**, but in a place where Member State law applies by virtue of public international law.

Other countries...

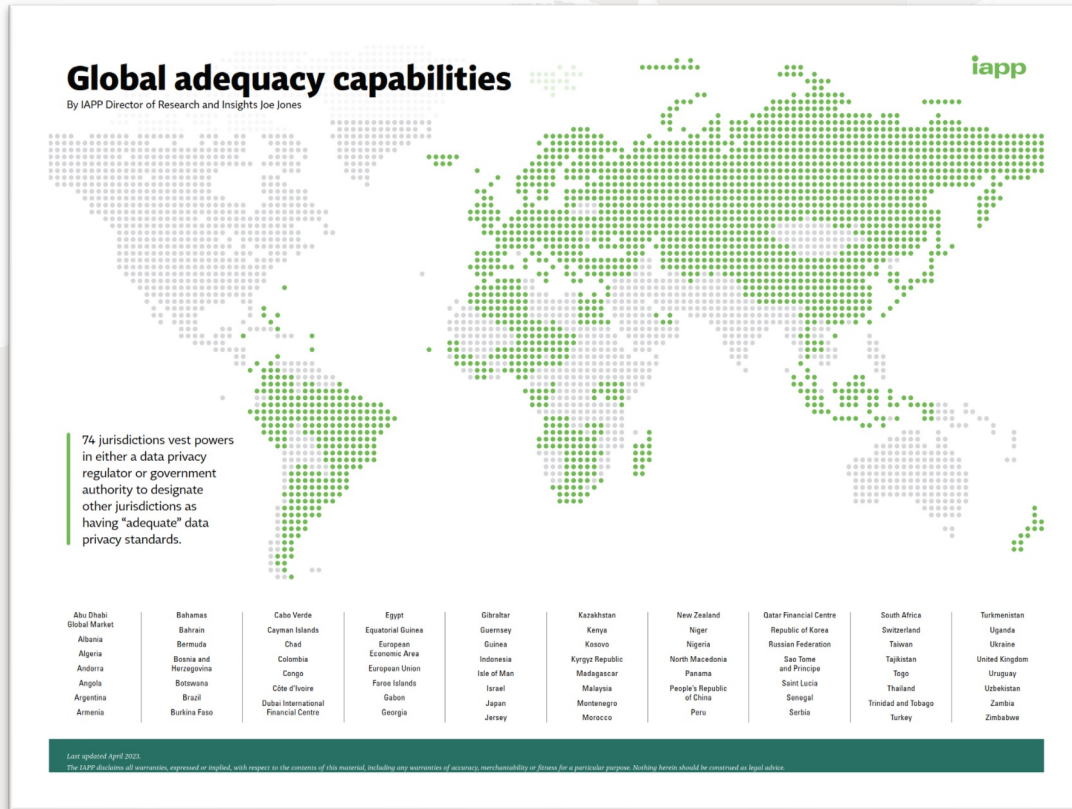


Data privacy laws and regulations established by Asian entities



No harmonization
or aligned data
privacy standard?

IAPP: 74 jurisdictions requires other jurisdictions to have adequate data privacy standards



IAPP(International Association of Privacy Professionals)

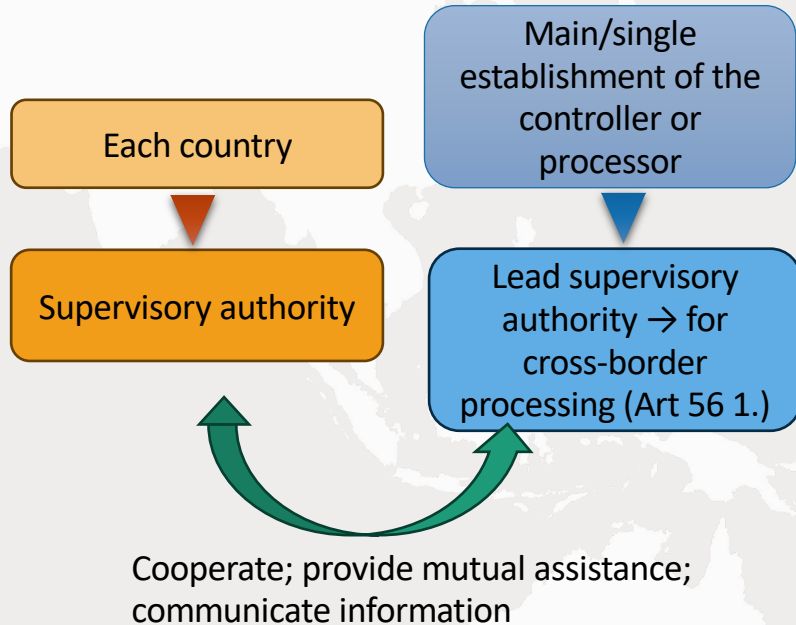
“An ‘adequate’ designation describes instances where a third country has been assessed as providing data privacy standards that are sufficiently comparable to those of the assessing jurisdiction. These unilateral determinations permit the free flow of personal data, without the parties to the transfer being required to implement further safeguards or obtain further authorizations.”

Sources: IAPP <https://iapp.org/resources/article/infographic-global-adequacy-capabilities/>

Take GDPR as an example...

Art 63. GDPR - Consistency mechanism:

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.



In the referenced Uber case, the French authority collaborated with the Dutch Data Protection Authority (DPA) to investigate Uber's breach of GDPR. The Netherlands assumes the role of the lead supervisory authority due to the presence of Uber's primary establishment in Europe.

Cooperation with the CNIL throughout the procedure

Under the procedures for cooperation between authorities introduced by the General Data Protection Regulation (GDPR), it was the Dutch data protection authority that was competent to conduct the investigations in this case, as Uber has its main establishment in the Netherlands.

The CNIL cooperated closely with its counterpart throughout the procedure, as part of the checks and analysis of the evidence obtained, and then when examining the draft decision as part of the one-stop shop procedure.

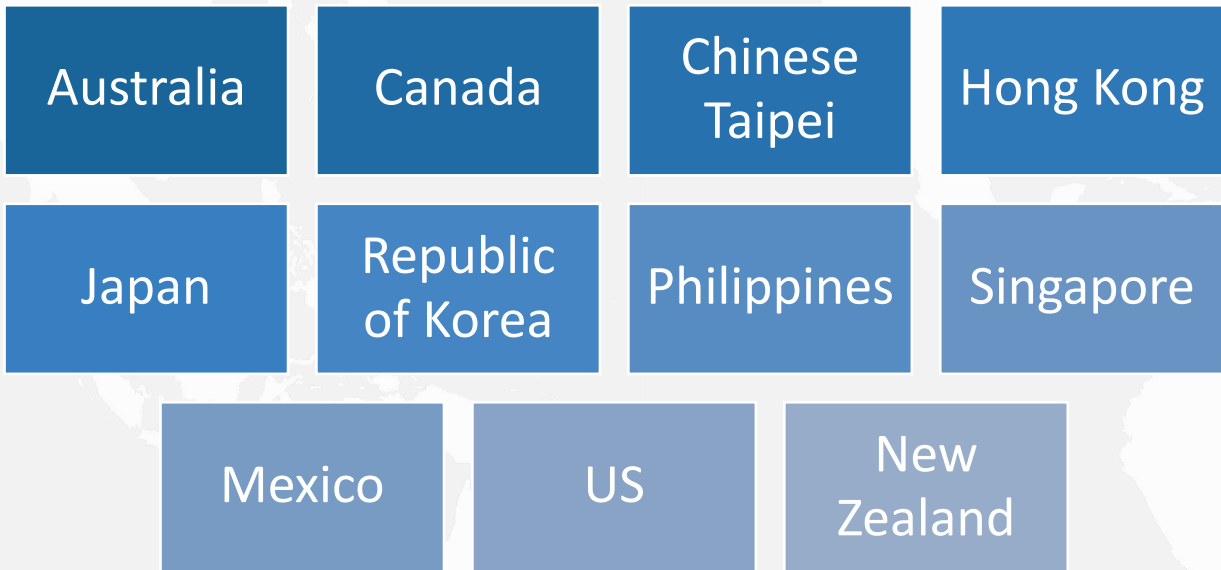
Sources: CNIL <https://www.cnil.fr/en/uber-dutch-data-protection-authority-imposes-eu10-million-fine>



Without a cross-border standard in addressing data privacy, it will be challenging for countries to cooperate and set out an aligned practice.

- APEC Cross-Border Privacy Rules (CBPR) System
- A voluntary, accountability-based system that facilitates privacy-respecting data flows among APEC economies. It is a crucial component of APEC's efforts to promote the development of the digital economy.
- CBPR, through its participation in APEC, establishes a requirement for international consistency in **privacy law compliance**. This is achieved by designated “Accountability Agents” (AAs) in each country, who verify businesses or organizations.
- CBPR certification serves as evidence of an enterprise or organization's commitment to and capability in managing data or personal information. It establishes a trusted environment for compliant data flows, thereby facilitating international business trade.
- Companies obtained CBPR certifications: Apple Inc. 、 GE 、 EA 、 Cisco 、 IBM 、 MasterCard 、 Virgin Pulse 、 World Wrestling Entertainment 、 Alibaba Cloud (Singapore) 、 Paidy(Japan).....
(<https://cbprs.org/compliance-directory/cbpr-system/>)

Participation: 27 participating “Privacy Enforcement Authorities (PEA)” from 11 APEC economies



Organization shall fill in CBPR's **questionnaire** to evaluate its data privacy policies and practices.

The questionnaire can be divided into 8 sections, each with different requirements:

- Notice
- Collection limitation
- Use of personal information
- Choice
- Integrity of personal information
- Security safeguards
- Access and correction
- Accountability

5. How do you obtain personal information:

a) Directly from the individual?

Y N

b) From third parties collecting on your behalf?

Y N

c) Other. If YES, describe.

Y N



**Asia-Pacific
Economic Cooperation**

**APEC CROSS-BORDER PRIVACY RULES SYSTEM
INTAKE QUESTIONNAIRE**

39. What measures does your organization take to ensure compliance with the APEC Information Privacy Principles? Please check all that apply and describe below.

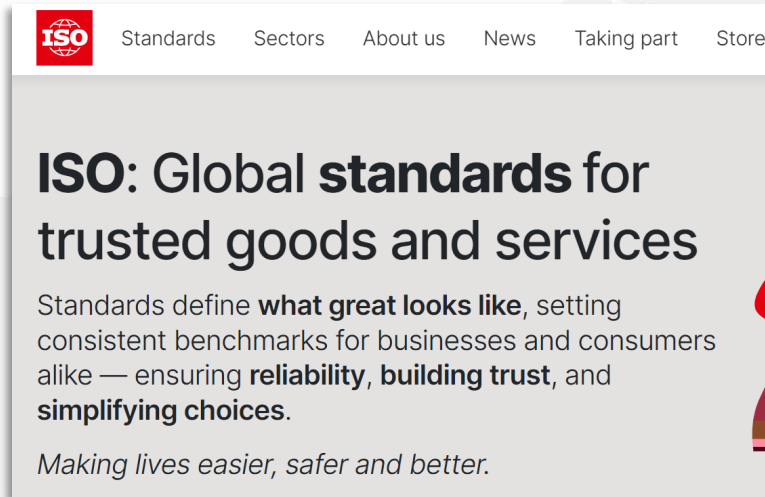
- Internal guidelines or policies (if applicable, describe how implemented) _____
- Contracts _____
- Compliance with applicable industry or sector laws and regulations ____
- Compliance with self-regulatory organization code and/or rules ____
- Other (describe) ____

40. Has your organization appointed an individual(s) to be responsible for your organization's overall compliance with the Privacy Principles?

Y N

Other data privacy standard —

ISO 27701: The Privacy Information Management Standard



ISO Standards Sectors About us News Taking part Store

ISO: Global standards for trusted goods and services

Standards define **what great looks like**, setting consistent benchmarks for businesses and consumers alike — ensuring **reliability, building trust, and simplifying choices**.

Making lives easier, safer and better.



ISO/IEC 27701:2019

Security techniques

Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management

Requirements and guidelines

A global framework for privacy information management system (PIMS), taking into account requirements of a myriad of laws and regulations, including GDPR.



Forecast on the future of Data Privacy

With the advancement of technology, the circulation of information has transcended border. Platforms and software that operate across borders, such as TikTok, travel website like Agoda, international hotel like Marriott, as well as cloud sharing platforms like Dropbox and Google Drive, all have the possibility to access personal or sensitive information from users, which highlights the importance of unified personal data standards to ensure aligned data protection.



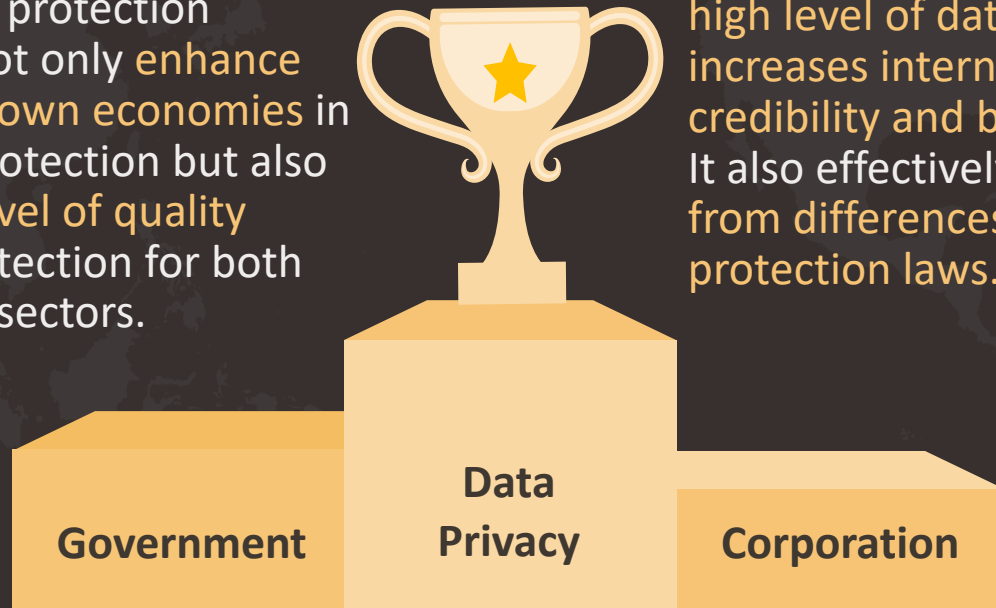
The forecast

- The increased in fines and General Public's awareness
- The increase in AI legislation world wide
- Increase in Data controlling right awareness: 1. The expansion of data localization due to the emerging privacy laws requires company to control the data in the country in which it resides. 2. Consumers demand greater control over their own data—the right to own and manage personal information
- the massive use of raw data/unstructured data.
- More data accountability privacy-enhancing technology (PET) for data management

Collaboration and harmonization would be the best way

If governments are able to cooperate with each other and achieve a certain consensus on data protection measures, it will not only enhance the image of their own economies in the field of data protection but also ensure a certain level of quality control in data protection for both public and private sectors.

The implementation of CBPR demonstrates that companies have a high level of data protection, which increases international market credibility and business opportunities. It also effectively reduces risks arising from differences in international data protection laws.





Thank you

Formosan Brothers is a full service law firm founded in 1997 in Taiwan. For the past 27 years, our expertise covers a wide range of laws. We assist our client by cooperating with foreign firms located in more than 120 countries.



Taipei Office

16F-6, No. 376, Sec. 4,
Ren-Ai Rd., Da'an,
Taipei, 106434 Taiwan
TEL : +886-2-2705-8086



Hsinchu Office

5F, No. 249, Dong Sec. 1,
Guangming 6th Rd.,
Zhubei, Hsinchu 302044,
Taiwan
TEL : +886-3-550-1508



Taichung Office

5F-5D, No. 186, Shizheng
N. 7th Rd., Taichung
407612, Taiwan
TEL : +886-4-2251-2886

Website



People

