28.08.2024

Third Country Assessment / Transfer Impact Assessment

Google Workspace for Education in Taiwan

Et bilde som inneholder symbol, logo, design

Automatisk generert beskrivelse

[1. Introduction 3](#_Toc176427830)

[1.1. Description of the Transfer and the Purpose of the Country Assessment 3](#_Toc176427831)

[1.2. Legal Framework 3](#_Toc176427832)

[1.3. Other Sources 3](#_Toc176427833)

[1.4. Limitations and Reservations 4](#_Toc176427834)

[2. Summary and Conclusion 4](#_Toc176427835)

[3. Description of Relevant Regulations in Taiwan 4](#_Toc176427836)

[3.1. Personal Data Protection Act (PDPA) 4](#_Toc176427837)

[3.2. Communication Security and Surveillance Act (CSSA) 6](#_Toc176427838)

[3.3. Telecommunications Act and Telecommunications Management Act 8](#_Toc176427839)

[4. Country Assessment - Taiwan 9](#_Toc176427840)

[4.1. Overall Issue and Method 9](#_Toc176427841)

[4.2. Regulations Applicable to the Transfer to Taiwan 10](#_Toc176427842)

[4.3. Evaluation of the Applicable Laws for the Transfer 11](#_Toc176427843)

[4.4. How the Relevant Laws Are Enforced in Practice 14](#_Toc176427844)

[4.5. Summary of Practices 18](#_Toc176427845)

[5. Conclusion and Recommendation 19](#_Toc176427846)

[References 20](#_Toc176427847)

[Questions and Answers from Local Expertise at Nishimura & Asahi Taiwan Law Firm 22](#_Toc176427848)

***Disclaimer***

This raport was translated from Norwegian to English using the AI-based language model ChatGPT-4o on september 4th 2024.

Please note that while the translation aims to be accurate, it may not fully reflect all nuances of the original text. Human oversight has not been applied to this translation process.

# 1. Introduction

## 1.1. Description of the Transfer and the Purpose of the Country Assessment

Norwegian municipalities use cloud services under Google Workspace for Education ("GWE") in primary schools. This means that personal data on students, parents, and staff is processed. The use of Google services involves data transfers to or remote access from countries not covered by an adequacy decision from the European Commission under GDPR Article 45.

The use of GWE means that Google stores data on servers in Taiwan. The transfers concern personal data on Norwegian users of Google Workspace for Education, including students, teachers, and parents. The transfers will take place continuously. Personal data is processed locally and on data servers in Norway/EU but may be transferred to Taiwan for storage purposes (cloud storage where the data is physically located on a server in Taiwan).

The municipality is the data controller for these transfers and must assess the risk involved in the transfers, as well as enter into the necessary Standard Contractual Clauses ("**SCC**") published by the European Commission and conduct a Transfer Impact Assessment ("**TIA**") with the implementation of necessary security measures for the transfers if the SCCs alone are not sufficient.

This country assessment is intended to guide municipalities in assessing the protection level and security measures in Taiwan so that the municipality can conduct a TIA. To assess the protection level of the transfers, the municipality must evaluate the laws and legal practices of the importing country. This country assessment reviews relevant legislation in Taiwan that affects the privacy of Norwegian data subjects.

## 1.2. Legal Framework

The primary laws regulating government access to personal data in Taiwan are:

* **Personal Data Protection Act (PDPA)**, see section 3.1.
* **Communication Security and Surveillance Act (CSSA),** see section 3.2.
* **Telecommunications Act (TA) and Telecommunications Management Act (TMA),** see section 3.3.
* **Constitution or other related treaties and conventions.**

In addition, the **Code of Criminal Procedure (CCP)** and the **Police Power Exercise Act (PPEA)** are mentioned but are not evaluated in detail below.

## 1.3. Other Sources

**DataGuidance/DataGovernance**: DataGuidance is a centralized regulatory research platform built by a network of internal researchers, legal experts, and translators.[[1]](#footnote-2)

**"Taiwan Internet Transparency Report"**: A research report published by the Taiwan Association for Human Rights.[[2]](#footnote-3)

**Other**: Additional professional literature, articles, and other relevant sources (see footnotes).

## 1.4. Limitations and Reservations

This country assessment covers only the regulations and practices that were publicly available or known to the project and relevant to the evaluations.

We also note that legal sources and practices may have been updated, changed, or phased out since the country assessment was made available.

The conclusions in this country assessment are based on the project's interpretation and assessment of Taiwanese law and practices.

## 2. Summary and Conclusion

The country assessment provides an evaluation of Taiwan's legislation and practices concerning privacy and surveillance, particularly in light of Norwegian schools' use of Google Workspace for Education (GWE). The main findings indicate that, although Taiwan has made several legislative changes to enhance privacy protection, challenges remain related to surveillance and data protection.

It has been identified that the Communications Security and Surveillance Act (CSSA) does not fully meet fundamental European guarantees, particularly regarding independent oversight and effective legal remedies. This could affect the level of protection for personal data transferred to Taiwan.

The project recommends that municipalities using GWE assess the risks of transfers to Taiwan and implement the necessary security measures. This may include entering into Standard Contractual Clauses (SCCs) and conducting a Transfer Impact Assessment (TIA).

Furthermore, attention should be paid to the enforcement of the legislation, as indicated by the report from the Taiwan Association for Human Rights (TAHR) and Google’s Transparency Reports, which suggest shortcomings.

Finally, the country assessment concludes that additional measures are needed to ensure an adequate level of protection for personal data transferred to Taiwan.

# 3. Description of Relevant Regulations in Taiwan

## 3.1. Personal Data Protection Act (PDPA)

### 3.1.1. Scope of the Law

The Personal Data Protection Act governs the protection of personal data in Taiwan. All collection, processing, and use of personal data in Taiwan are subject to the PDPA and its “Enforcement Rules”.[[3]](#footnote-4) The law came into effect in 2015. Taiwan is not covered by an adequacy decision from the European Commission.

According to Article 51, paragraph 2 of the PDPA, combined with the interpretation from the competent authority (FA-Lu-Zi No. 10403509750 dated 26 August 2015), the PDPA covers all collection, processing, and use of personal data within Taiwanese territory, regardless of whether the data subjects are located in Taiwan.[[4]](#footnote-5)

Processing of personal data means recording, inputting, storing, compiling/editing, correcting, duplicating, retrieving, deleting, outputting, or connecting. Use of personal data refers to the handling of personal data through any methods other than those mentioned under the term "processing."

The transfer of personal data concerning Norwegian users of GWE to a data center in Taiwan will, therefore, constitute processing of personal data covered by the PDPA.

### 3.1.2. Government Access to Transferred Data

Chapter 2 of the PDPA regulates the collection and handling of data falling outside the provisions of Chapter 1. This includes, among other things, the collection of data necessary for national security or law enforcement purposes.

Articles 15 and 16 set the framework for such processing. Article 15 permits the processing of personal data outside Chapter 1 only if one of three conditions is met: necessary for a statutory obligation of the state, consent, or the rights and interests of the data subject are not infringed. Article 16 sets out the legitimate purposes for such processing, the most relevant being that the processing is mandated by law or necessary for national security or public interest. Both Articles 15 and 16 refer to other national laws generally. We refer to section 1.2 above for an overview and further assessments below.

Private companies and organizations cannot oppose requests for access to or collection of data by state authorities. However, organizations can file a complaint with the competent authority if they believe the request is unlawful. If a complaint is unsuccessful, the organization can appeal the case to the relevant national court or quasi-judicial body. The wording is otherwise silent on the scope and limits of the Taiwanese authorities' powers to collect data.

### 3.1.3. Legal Basis for Processing

Under Chapter 1 of the PDPA, the state’s access to personal data is limited to cases where the following conditions are met:

1. It is necessary to fulfill a statutory obligation of the state.
2. Consent has been obtained from the individual (data subject).
3. The rights and interests of the data subject are not infringed.

### 3.1.4. Principles, Rights, and Other Restrictions on the Processing of Personal Data

The PDPA includes overarching principles for compliance with the law. These principles are listed in various provisions.[[5]](#footnote-6) The principles include requirements for proportional, adequate, and relevant data processing; purpose limitation, necessity, and proportionality of the processing; special rules for sensitive personal data; and other principles similar to those found in the GDPR.[[6]](#footnote-7)

### 3.1.5. Enforcement, Oversight, and Review of Rights

There is no dedicated independent supervisory authority comparable to European data protection authorities. However, later amendments to the PDPA have formalized the establishment of such an authority. This authority will be called the Personal Data Protection Commission (PDPC) but is not yet operational in practice.[[7]](#footnote-8)

The National Development Council (NDC) is responsible for enforcing and issuing decisions on matters within the scope of the PDPA, as well as interpreting both the PDPA and the internal procedures that public bodies are required to establish under the PDPA.

### 3.1.6. Approach to GDPR and Adequacy Decision

The PDPA has undergone several amendments since its implementation in 2015. Some of these changes may have been influenced by European law, particularly the GDPR.[[8]](#footnote-9) It appears that Taiwanese authorities have an ambition to achieve an adequacy decision from the EU.[[9]](#footnote-10) Since 2015, several public hearings have been held with the goal of improving the PDPA in a democratic manner.[[10]](#footnote-11) It is not known to the project whether, or at what stage, the EU is in the process of recognizing Taiwan as a lawful importer of personal data.

## 3.2. Communication Security and Surveillance Act (CSSA)

### 3.2.1. Scope of the Law

The Communication Security and Surveillance Act ("CSSA") authorizes governmental surveillance of communications deemed relevant to police or other governmental investigations.

The purpose of the law is as follows:

"This Act is enacted to safeguard the freedom of private communications and privacy, to protect from unlawful intrusion, and to ensure national security and maintain social order." (cf. Article 1)

Under Article 13, surveillance should be conducted by "intercepting, wiretapping, sound recording, video recording, photographing, opening, checking, copying communications or other similar necessary methods [...]." The CSSA does not provide clear guidance on the distinction between targeted surveillance and bulk data collection or the legal basis for this.

### 3.2.2. Government Access to Transferred Data

Surveillance under the CSSA is not limited to information about or communications between residents of Taiwan. Under Article 7, the target of a specific surveillance activity can be:

* "Domestic communications of foreign forces, hostile foreign forces, or their agents,"
* "Cross-border communications of foreign forces, hostile foreign forces, or their agents,"
* "Offshore communications of foreign forces, hostile foreign forces, or their agents."

The term "foreign forces" is defined in Article 8 and includes:

* "Foreign governments, foreign or overseas political entities, their subordinate organizations or representative agencies,"
* "Organizations under the direction or control of foreign governments, foreign or overseas political entities,"
* "Organizations with the aim of operating international or cross-border terrorist activities."

The term "agent of foreign forces or offshore hostile forces" is defined in Article 9 as:

* "A person who participates, coerces others, or abets others in gathering secret intelligence, or other secret intelligence activities for foreign forces or offshore hostile forces, that risk endangering national security,"
* "A person who participates, coerces others, or abets others in sabotage or cross-border terrorist activities for foreign forces or offshore hostile forces,"
* "A person who serves as an official, or an employee for foreign forces or offshore hostile forces, or as a member of an international terrorist organization."

### 3.2.3. Legal Basis for Processing

Surveillance under the CSSA requires several legal conditions to be met. Under Article 5(1) of the CSSA, surveillance must be directed towards "communications" or "communications records." "Communications" means "[u]tilizing wired and wireless telecommunication equipment to send, store, transmit, or receive symbols, texts, images, sound, or other types of information" (cf. Article 3, no. 1). This includes mail and letters, as well as speeches and conversations (cf. nos. 2 and 3). "Communications records" refers to data types such as metadata, which in Article 3-1 is described as "records such as the telecommunications numbers of the sender and the recipient, time of communication, length of use, address, service type, mailbox or location information generated by the telecommunications system after the telecommunications user uses the telecommunications services."

Based on the wording of Article 5, the CSSA covers most data that would naturally fall under the concept of communications, including both digital and analog communications. Authorization for surveillance is only granted in cases of criminal or law-enforcement investigations under Taiwanese law.[[11]](#footnote-12)

### 3.2.4. Principles, Rights, and Other Limitations

Surveillance must be necessary and proportional. Article 2 stipulates that: "The surveillance mentioned in the preceding Paragraph shall not exceed the necessary limits to achieve the objective, and the appropriate methods for the action should have only the minimum intrusion."

### 3.2.5. Enforcement, Oversight, and Review of Rights

Under Article 5(2), no surveillance can be initiated without approval or an "interception warrant" from "the court." It is unclear which court or judicial authority the term "the court" refers to. However, it is assumed that this includes all ordinary courts in Taiwan that have jurisdiction over criminal matters. More on judicial oversight is addressed in section 4.

## 3.3. Telecommunications Act and Telecommunications Management Act

### 3.3.1. Scope of the Law

The Telecommunications Act ("TA") came into effect in 1996 but was later replaced by the Telecommunications Management Act ("TMA") in July 2020.[[12]](#footnote-13) The purpose of the legislation was to ensure the safe development of telecommunications, promote public welfare, protect communications, and safeguard the rights and interests of telecommunications users in Taiwan.[[13]](#footnote-14)

The TMA continues and expands upon the purposes of the TA. This also applies to large portions of the TA's other provisions. Despite the continuity, the introduction of the TMA is considered a significant legal change in Taiwan. Of particular interest to this project are the changes to the legal bases for disclosure requests from state authorities under the TA.

### 3.3.2. Government Access to Transferred Data under the TA

Article 7 of the TA states that a "telecommunications enterprise or its employees, including the retired, shall hold the existence and contents of communications in strict confidence."

The wording suggests a general rule that data obtained and stored in connection with the use of electronic tools in Taiwan must be archived and secured. Exceptions to this general rule are triggered when "the disclosure of such records" is carried out in accordance with applicable laws and regulations. Which applicable laws and regulations these are is not specified. However, it can be assumed that this is an implicit reference to the CCP and CSSA, as in the PDPA.

Article 3 of the "Regulation for Handling Requests from Competent Authorities for Comm. Rec." is also relevant in this context. According to J. Marshall, the criteria for disclosure involve a "‘[...] easy-to-meet’ standard that only requires the applicant agency to state the necessity, reasonableness, and proportionality when requesting the records."[[14]](#footnote-15) The project is unable to verify whether this understanding is correct, as the mentioned regulation is no longer available, likely due to the TA being replaced by the TMA in 2020.

### 3.3.3. Government Access to Transferred Data under the TMA

The general rule on the archiving and protection of "records" has been carried over into the TMA, albeit with a slightly different wording (see Article 7 in the TA above). The TMA does not appear to retain the exception regarding disclosures to state authorities. Exceptions to the general rule may still occur, but the conditions have been altered. With respect to the disclosure of data to state authorities, reference is made to the relevant provisions and exceptions in the CSSA (see Article 9, final paragraph). It states: "Telecommunications enterprises and those who have established PSTN are obliged to assist in the implementation of communication surveillance and in the access of communications records and communications user’s information in accordance with the Communication Security and Surveillance Act."

# 4. Country Assessment - Taiwan

## 4.1. Overall Issue and Method

According to Step 3 of the EDPB's "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0," the purpose of a country assessment is to determine whether there are laws and/or practices in the country to which personal data is being transferred that affect the effectiveness of the chosen transfer mechanism.[[15]](#footnote-16) The analysis should focus on local laws and regulations that are relevant to the transfer and the legal basis for the transfer. In relation to the specific transfer, the following question must be answered:

* Can the data importer guarantee an adequate level of protection for personal data transferred to the third country (Taiwan)?

Whether a third country can be considered to provide an adequate level of protection depends on:

1. Whether local surveillance laws apply to the specific transfer, and if so;
2. Whether the so-called "fundamental European guarantees" are met for government access to personal data under the relevant laws.[[16]](#footnote-17)

The fundamental European guarantees are based on the EU Charter as interpreted by the EU Court of Justice. These reflect, among other things, the fundamental right to privacy, which is also enshrined in Article 8 of the European Convention on Human Rights ("ECHR") and incorporated into the Constitution.

According to the EDPB, the four categories of fundamental guarantees can be described as follows:

* **Guarantee A**: The processing (access) must be based on clear and precise rules that are publicly available.
* **Guarantee B**: The processing (access) must be necessary and proportionate to achieve a legitimate purpose.
* **Guarantee C**: There must be an independent oversight body that can review the use of access.
* **Guarantee D**: The data subjects must have access to effective remedies if their rights are violated as a result of government access.

If all four categories of guarantees are in place, personal data is adequately protected during a transfer. If at least one of the guarantees is missing, additional measures must be implemented to provide an adequate level of protection for the personal data.[[17]](#footnote-18)

The country assessment also includes a review of how the regulations are implemented and enforced in practice. Practices will be used in this country assessment for two different purposes, depending on whether the fundamental guarantees are deemed to be met. If the laws being assessed do not meet the fundamental guarantees, the description of practices will be used as a factual basis for identifying appropriate compensatory security measures. If the laws being assessed meet the fundamental guarantees, the description of practices will be used to verify that the laws are actually enforced as stated.

## 4.2. Regulations Applicable to the Transfer to Taiwan

### 4.2.1. Communications and Surveillance Act (CSSA)

It is undisputed that personal data stored on Norwegian users at a data center in Taiwan is covered by the concept of communications as defined in Article 3, 3-1 of the CSSA. It is also clear that Norwegian users of GWE are covered by the term "Foreign Forces" in Article 8.

The project assumes that the CSSA may apply to data on Norwegian users of GWE stored in Taiwan.

### 4.2.2. Telecommunications Act (TA) and Telecommunications Management Act (TMA)

The TMA and TA contain provisions aimed at ensuring the state's ability to access communications and other data for various state investigations and/or surveillance processes. In practice, this involves mandatory assistance and the provision of systems and infrastructure so that communications and data can be shared. In the following, the TMA and TA will be assessed equally.

In this context, "telecommunication enterprises" or telecommunications operators are the obligated parties under the TMA and TA. The term telecommunications operator includes entities registered in accordance with the "Act to provide telecommunications services" and providing "telecommunications services."

Telecommunications services are further limited to telecommunications transmitted via the "PSTN" (Public Switched Telephone Network) - translated to the public switched telephone network (mobile and fixed telephone networks). PSTN constitutes the physical telecommunications infrastructure. The project sees PSTN as a fixed-line-based traditional telephony service, not a cloud storage service. The project believes that the specific service configuration of Google Workspace for Education in Norwegian schools does not qualify as PSTN in Taiwan.

Therefore, the use of Google Workspace for Education with cloud storage in Taiwan will fall outside the scope of the law. Local expertise in Taiwan at the law firm Nishimura & Asahi Taiwan supports this interpretation, see appendix.

The project concludes that the TMA and TA will not apply to personal data on Norwegian users of GWE stored in Taiwan.

## 4.3. Evaluation of the Applicable Laws for the Transfer

### 4.3.1. Communications and Surveillance Act (CSSA)

#### 4.3.1.1. Guarantee A: Clear and Precise Rules Publicly Available

The European Data Protection Board (EDPB) summarizes several key points when assessing the presence of the four guarantees. The guidance is based, among other things, on case law from the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR).[[18]](#footnote-19)

In assessing Guarantee A, the following questions and assessment criteria are relevant:

1. Are the legal grounds for surveillance sufficiently clear and precise regarding the scope and extent of the measures?[[19]](#footnote-20)
2. Is it sufficiently clear when surveillance can take place, including which situations and circumstances may legally trigger surveillance?[[20]](#footnote-21)
3. Are limitations on the ability of data subjects to assert their rights included and visible in the relevant legislation?[[21]](#footnote-22)
4. The requirements for precision and availability under point 1 must be assessed and applied equally across various government surveillance programs. Legal grounds for bulk data collection are therefore subject to the same clarity and precision requirements as legal grounds for targeted surveillance.[[22]](#footnote-23)
5. Are the individuals being surveilled able to foresee the consequences of an intervention under the relevant surveillance legislation? The requirement for foreseeable rules must reasonably be balanced against the need for secrecy and national security considerations.[[23]](#footnote-24)

The Communications and Surveillance Act aims to ensure free private communication, prevent unlawful intrusion, and protect national security and social order (project's translation, cf. Article 1). The law authorizes governmental surveillance of communications deemed relevant to police or other governmental investigations.

Regarding the scope and extent of the measures, Article 3 and Article 13 define the methods and scope of surveillance (see section 3.2.3 for details). Article 3-1 describes the extent of surveillance. Article 5 of the CSSA outlines the conditions under which a surveillance order may be issued. It refers to criminal provisions that are otherwise available.

Article 12 specifies the duration of surveillance initiated under Article 5 (surveillance based on criminal prosecution), Article 6 (surveillance based on election interference and threats to democracy), and Article 7 (surveillance based on foreign intelligence and espionage). The limitations on the rights of the data subjects are described throughout the CSSA.

#### 4.3.1.2. Guarantee B: Necessary and Proportionate for Achieving a Legitimate Purpose

Article 2 requires that any surveillance must be necessary, proportionate, and purposeful. However, it is unclear how this specifically limits the government's discretionary powers. Similar formulations of necessity, proportionality, and purposefulness are also included in other parts of the law where these requirements are naturally emphasized.

#### 4.3.1.3. Guarantee C: Independent Oversight and Review (Judicial Oversight)

There is no dedicated independent oversight body for the enforcement of the CSSA.

An "enforcement authority" must submit at least one report every 15 days during the course of communication surveillance to the prosecutor or judge who issued the surveillance order. The report must include the status of progress as well as an explanation of whether the surveillance should be continued.

Under Article 16-1, the "enforcement authority" and the "supervisory authority" must prepare an annual report with relevant statistics on the previous year's surveillance activity.

Article 32-1 further states that "The Ministry of Justice" must conduct annual audits of "the status of the enforcement of communications surveillance." The findings must be reported to the "Legislative Yuan," a judicial committee organized under the Taiwanese congress elected through democratic processes.[[24]](#footnote-25)

The CSSA does not describe an independent supervisory and oversight body. It is also important to note that, as mentioned in section 3.1.5, there is currently no dedicated, independent, and supervisory authority comparable to European data protection authorities under the PDPA. However, later amendments to the PDPA have formalized the establishment of such an authority. This authority will be called the Personal Data Protection Commission (PDPC) but is not yet operational.[[25]](#footnote-26) According to local expertise, a "preparatory office" for the PDPC was established on 5 December 2023, and the PDPC is expected to be operational by August 2025.

The National Development Council (NDC) is responsible for enforcing and issuing decisions on matters within the scope of the PDPA, as well as interpreting both the PDPA and the internal procedures that public bodies are required to establish under the PDPA.

#### 4.3.1.4. Guarantee D: Effective Remedies

The presence of effective remedies presupposes, among other things, that data subjects are able to assert their rights. Whether, and to what extent, data subjects are notified of initiated or completed surveillance is therefore of great importance, according to the EDPB.

Article 15 of the CSSA outlines the government's responsibility to notify individuals being surveilled. It specifies, among other things, that unless notification of the completed surveillance conflicts with the original surveillance purpose, "The court" must inform the individual(s) being surveilled within 14 days after the surveillance is completed. Article 15 also specifies the content requirements for such a notification.

"The court" is not given further description in the CSSA regarding its responsibilities, independence, competence, or other matters. However, a reasonable conclusion is that "the court" must be a court or other competent authority with the power to issue decisions in criminal cases, as the legal basis for surveillance under the CSSA largely presupposes a criminal act under national law (see Articles 5 and 7).

According to the EDPB, there is no requirement that "the court" must be a formal court. As long as cases can be brought before a "national authority" or "body" offering the guarantees mentioned in Article 47 of the Charter, this should be sufficient.[[26]](#footnote-27) It is also important that the relevant body has the authority to issue binding decisions on the national surveillance and intelligence services. On this point, it is unclear whether "the court" is granted such authority in Taiwan.

Regarding the use and enforcement of applicable remedies, Article 24 of the CSSA states that illegal surveillance is punishable by "fixed-term imprisonment" of up to five years. Illegal disclosure of confidential or other types of information obtained under the CSSA is also punishable by "fixed-term imprisonment" of up to five years.

The CSSA does not offer immediate enforcement of rights or remedies if illegal surveillance is conducted. This is because secrecy is a fundamental part of any surveillance action, making it difficult to enforce rights during the surveillance process.

Finally, it is worth noting that the PDPA allows for both administrative and legal processes for data subjects whose data has been disclosed ("transferred").[[27]](#footnote-28) Under certain circumstances, the PDPA grants data subjects the right to object to processing, review, revise, supplement, or delete their personal data. However, this point is only relevant to the extent that the remedies mentioned in the PDPA can also be applied to surveillance under the CSSA, which is uncertain.

#### 4.3.1.5. Conclusion

The project's assessment is that the CSSA does not meet the fundamental European guarantees. This applies to Guarantees C and D. As a result, the project must consider the need for additional supplementary measures to ensure an adequate level of protection for the transfer of personal data.

## 4.4. How the Relevant Laws Are Enforced in Practice

The project further assesses how the relevant laws applicable to the transfer are enforced in practice.

According to the EDPB's guidance, an analysis of the third country's practices can help verify the evaluation of the laws against the fundamental guarantees. Since the CSSA does not meet the fundamental guarantees, it is not necessary to consider and weigh practice in this way. However, the project chooses to include a description of practice because it is relevant to identifying supplementary security measures in the next step of the TIA.

The following section contains a review of practices from the PDPA, CSSA, Google, and the "Taiwan Internet Transparency Report" provided by the Taiwan Association for Human Rights. Finally, a summary of the dialogue with local expertise in Taiwan is presented.

### 4.4.1. Case Law

#### 4.4.1.1. The Court System in Taiwan

"Judicial Yuan" is a branch of the central government and constitutes the judicial system in Taiwan. The responsibility for and operation of the Taiwanese Constitutional Court is entrusted to the "Judicial Yuan," along with other parts of the functioning legal system, including ordinary courts, appellate courts, district courts, the Supreme Court, and more.

The Constitutional Court consists of 15 judges appointed by the President of Taiwan. The judges cannot take office without the consent of the "Legislative Yuan," which is the legislative body in Taiwan. The appointment of Constitutional Court judges appears to be subject to oversight by both the legislative and executive branches, giving the selection process a somewhat political nature.

#### 4.4.1.2. PDPA

There are several examples of court decisions regarding the PDPA and related laws in Taiwan. These are rulings issued by the Supreme Administrative Court, the Taiwan High Court, and the Taipei District Court.[[28]](#footnote-29) These rulings primarily address the enforcement and compliance with rights under the PDPA, particularly balancing these rights against state interests and considerations.

The project has not identified any court decisions related to the PDPA that are relevant to this analysis. This is because the PDPA, as the project sees it, does not protect Norwegian users of GWE located in Norway. Therefore, we will not discuss the PDPA further in this country assessment.

#### 4.4.1.3. Case No. 631

The Taiwanese Constitutional Court has published an "interpretation" (hereafter referred to as Interpretation No. 631 from 2007) titled "Issuance of Communications Surveillance Warrants Case." The Constitutional Court is part of the Taiwanese "Judicial Yuan." The interpretation concerns the application of Criminal Judgment 92-Shang-Su-882 (2003), which was issued by the Taiwan High Court.[[29]](#footnote-30)

The interpretation addresses the constitutionality of Article 5, paragraph 2 of the CSSA in relation to Article 12 of Taiwan's Constitution on "freedom of secrecy of correspondence." It is regarded in Taiwan as an authoritative interpretive contribution to the enforcement of the law, both for ordinary law enforcement agencies in Taiwan and for other courts.

The case involved the surveillance of a phone conversation between a Taiwanese police officer and Ms. X, during which the police officer, at Ms. X's request, disclosed information about Ms. KAO from the prosecutor's office database. The disclosure of information was illegal under Taiwanese criminal law, but because a police order for surveillance under Article 5, paragraph 2 of the CSSA does not require court approval, the police officer argued that the surveillance of the phone conversation violated Article 12 of the Taiwanese Constitution.[[30]](#footnote-31)

In its reasoning, the court describes the considerations and interests that should be taken into account when enforcing the CSSA. In its discussion of surveillance activities authorized under Articles 2, 5, and 7 of the CSSA, the court emphasizes that "[c]ommunications surveillance is essentially a measure that violates the people’s basic rights with extreme force and in a broad way. In order to achieve the purpose of the coercive measure, when conducting communications surveillance, the State usually deprives those who are put under surveillance of their rights to avoid such coercive measure before the measure is adopted."

Furthermore, the court highlights the importance of limiting "unnecessary violations of privacy rights that occur due to the coercive measure adopted by investigation authorities and at the same time not compromise the purpose of the coercive measure."

To limit the extent of the intrusion, the court emphasizes the necessity of establishing "an independent and impartial judicial institution in charge of reviewing government applications for communications surveillance warrants so that the people’s freedom of secrecy of correspondence can be protected."

In conclusion, the court found that Article 5, paragraph 2 of the CSSA, at that time (2007), violated the right to "secrecy of correspondence." As a result, Article 5, paragraph 2 was nullified.

Since 2007, several amendments have been made to Article 5, paragraph 2. The article now includes a provision that "[t]he interception warrant [...] shall be applied for, during the investigation, by the prosecutor upon receiving applications from judicial police authorities, or applied by the prosecutor ex officio to the court concerned for issuance." Based on this wording, it is now required that an application for a police order for surveillance must be routed through and approved by "the court concerned for issuance."

The court's interpretation indicates that ongoing assessments are made regarding the constitutionality of the legal basis for surveillance. The interpretation illustrates that the court weighs the nature and extent of the intrusion against established rule-of-law principles of judicial oversight and proportionality. The interpretation resulted in a legal amendment that implements a form of legality principle; the extent of the intrusion dictates the safeguards that are implemented. The legal framework also appears dynamic, as specific provisions can be subject to change based on rule-of-law principles or individual rights.

### 4.4.2. Taiwan Internet Transparency Report

The Taiwan Association for Human Rights (**TAHR**) published a report in 2015 titled "Taiwan Internet Transparency Report" (hereafter referred to as "**TITR**" or "**the report**"). The purpose of the report was to highlight the extent of intrusion into privacy and personal data protection in Taiwan. The report is the result of a research project conducted by TAHR. The findings are based on the period from 2012 to 2014. Although the report is from 2015, the numbers are likely still representative of the situation in Taiwan. The report is therefore considered relevant to the country assessment.

The report indicates that since 2010, Taiwanese authorities have significantly strengthened the country's technological surveillance capabilities.[[31]](#footnote-32) This has led to a substantial increase in wiretapping activities in Taiwan. TAHR further reports that compliance with rule-of-law principles regarding reasonable suspicion, due process, and independent oversight bodies is lacking. The report calls for greater transparency so that cases can be brought before open courts. In this context, the report's lead author, Ho Ming-syuan, states that "[...] a great number of device users had not been informed about the surveillance demands and were left in the dark," and adds that "[...] most authorities simply skipped the legal procedures by writing to the operators, asking for information they wanted."[[32]](#footnote-33)

The report presents statistics on requests for data access or disclosure submitted by various government agencies. The statistics show which specific laws and provisions the requests were based on. It reveals that a large proportion of the requests were based on the CSSA. This applies across different government agencies (see Coast Guard Administration and National Police Agency).[[33]](#footnote-34)

The report also categorizes surveillance requests based on purpose. Under "Overview on reasons for internet personal data requests in 2012-2014," the report indicates that between 2012 and 2014, 3,765 out of 4,908 (76%) requests were justified by criminal investigations. These figures are based on feedback from only seven of the 14 agencies that were asked to provide statistics. The total number of requests (4,908) reported is therefore likely not a complete picture of surveillance activities in Taiwan between 2012 and 2014.

As mentioned in section 4.3.1.3, Article 16-1 of the CSSA requires that the "enforcement authority" and "supervisory authority" prepare an annual report with relevant statistics on the previous year's surveillance activity. In 2015, the TITR project requested access to this report, and the "Department of Statistics of the Judicial Yuan" granted access and made statistics available for the second half of 2014. The statistics were divided into eight categories (lines) of communication surveillance:

1. Local telephone and mobile surveillance,
2. IMEI ("International Mobile Equipment Identity"),
3. IMSI ("International Mobile Subscriber Identity"),
4. HiNet ADSL accounts,
5. Internet telephone accounts (e.g., Skype),
6. Email addresses,
7. IP addresses,
8. Other.

In the second half of 2014, 14,292 requests for communication surveillance were submitted across 21,125 lines. Of the total 14,292 requests, 89.31% (12,841) concerned surveillance of local telephone and mobile networks.[[34]](#footnote-35)

The statistics are incomplete in several areas. According to the report, significant dark figures are likely. When comparing statistics from the Judicial Yuan with statistics made available or provided by organizations that received requests for access or disclosure of data, significant discrepancies were revealed. The report highlights several factors that may contribute to this:

* **Lack of specific numbers**: Of the 14 government agencies in Taiwan that were asked to provide information, only seven responded.
* **Lack of guidelines and procedures**: According to the report, only the "Criminal Investigation Bureau" could confirm that procedures had been established for systematizing statistics on their operations. It can therefore be concluded that the lack of clear guidelines and procedures for maintaining statistics at the various government agencies is a recurring challenge.[[35]](#footnote-36)
* **Lack of cooperation**: Several agencies either did not respond or opposed TAHR's request to share statistics.[[36]](#footnote-37)
* **Different understanding and perspective**: There seem to be significant differences in the definition of personal data across the actors TAHR contacted.
* **Legal gag order**: According to the National Security Bureau in Taiwan, the agency is legally prevented from sharing information under Article 16-1, paragraph 2 of the CSSA. This type of "gag order" likely applies to several other actors as well.[[37]](#footnote-38)

#### 4.4.2.1. Conclusion from the "Taiwan Internet Transparency Report (TITR)"

The report reveals several issues that are relevant to assessing how the CSSA is enforced in practice. However, two points are particularly important for evaluating the protection of personal data transferred to Taiwan:

1. According to the report, 89% of reported surveillance requests concerned local telephone and mobile networks. Since the use of GWE in Norwegian schools only involves data processing in the other service levels of the OSI model, it can be argued that the practical implementation of the CSSA does not significantly affect the transfer to Taiwan.
2. According to the report, 76% of all surveillance requests between 2012 and 2014 were made as part of a criminal investigation. The project draws the following conclusion from this: To the extent that surveillance occurs in Taiwan, it is highly likely that the surveillance is triggered by Taiwanese criminal law. This significantly narrows the scope of data that may be affected by government surveillance under the CSSA.

### 4.4.3. Google

#### 4.4.3.1. Google's "Transparency Reports"

Google regularly publishes reports with statistics on global requests for user information. The reports are updated every six months. They provide data on the number and type of requests Google receives from government authorities.[[38]](#footnote-39)

Since January 2020 and through 2024, Google reports a total of 5,550 requests from Taiwanese authorities. On average, just over half of these requests resulted in the disclosure of data. The reports distinguish between "Emergency disclosure requests" and "Other legal requests." It is not clear what this distinction entails or which laws the requests are based on. The report provides only a quantitative overview of the situation from Google's perspective.

#### 4.4.3.2. Correspondence with Google

The project contacted Google to request information relevant to the country assessment. A written request was sent to Google on April 29, 2024, and a response was received on May 10, 2024. The request asked Google to describe its handling of data disclosure requests from Taiwanese authorities.

The project considers Google's response to be of limited value to the country assessment. Google referred to publicly available information in its "Transparency Reports." Only Google's reporting of statistics on disclosure requests related to GWE was relevant to the project. Google reported that it had received only four requests related to GWE in 2022. In light of the report from TAHR in section 4.4.2.1 (1), this suggests little to no change in the frequency and scope of surveillance since 2014. There is little reason to believe that the situation will change in the coming years.

### 4.4.4. Local Expertise in Taiwan

The project has been in dialogue with local expertise in Taiwan and has sent questions to the law firm Nishimura & Asahi Taiwan. The purpose is to verify that the project's interpretation of Taiwanese law aligns with current law in Taiwan. The questions include statements about Taiwanese law that needed to be confirmed or refuted.

Nishimura & Asahi supports the project's conclusions on key points. Responses from Nishimura & Asahi Taiwan, along with the project's questions, can be found in the appendix to this country assessment.

## 4.5. Summary of Practices

The review of practices provides an understanding of how the relevant laws for data transfer are enforced in Taiwan. The project follows the EDPB's guidance, which recommends analyzing the third country's practices to verify whether the laws meet the fundamental guarantees. Although the CSSA does not meet the fundamental guarantees, the description of practices is included to identify supplementary security measures in the TIA analysis.

The text provides a detailed review of case law, including a description of the "Judicial Yuan" and a case (Interpretation No. 631) concerning the legality of surveillance under the CSSA. This interpretation resulted in a law change requiring judicial oversight of surveillance requests.

The "Taiwan Internet Transparency Report" (TITR) from 2015 highlights increased surveillance activity and shortcomings in the rule of law in Taiwan. The report points to significant dark figures and a lack of transparency from Taiwanese authorities.

Google's "Transparency Reports" show that there have been relatively few requests for data disclosure from Taiwanese authorities. The project also corresponded with Google, which confirmed a limited number of requests related to GWE.

# 5. Conclusion and Recommendation

The country assessment shows that although Taiwan's laws and practices have been amended to improve legal certainty, there are still significant challenges regarding surveillance and transparency. In particular, most surveillance requests are related to criminal investigations and predominantly affect local telephone and mobile networks.

This suggests that the use of GWE in Norwegian schools is unlikely to be significantly affected by Taiwanese surveillance. However, there is uncertainty about the full extent of government intrusion into privacy, which requires the implementation of supplementary security measures.

Based on the analysis, it is advised not to transfer personal data to Taiwan due to significant concerns about the enforcement of the CSSA in practice and the lack of guarantees for privacy protection.

It is important to note that this is only a recommendation, and the final decision on whether to transfer personal data to Taiwan must be made by the individual organization based on its own assessment of the risks.

# References

**Legislation and Legal Documentation**

* Personal Data Protection Act (PDPA), <https://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021>
* Telecommunications Act (TA), <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=K0060001>
* Telecommunications Management Act (TMA), <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=K0060111>
* European Data Protection Board (EDPB), "Recommendations 02/2020 on the European Essential Guarantees for surveillance measures Adopted on 10 November 2020," 2020, <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf>
* Constitutional Court R.O.C (Taiwan), No.631 [Issuance of Communications Surveillance Warrants Case], 20.07.2007, <https://cons.judicial.gov.tw/en/docdata.aspx?fid=100&id=310812>
* Law on the Strengthening of Human Rights in Norwegian Law (Human Rights Act), Article 8, <https://lovdata.no/dokument/NL/lov/1999-05-21-30/KAPITTEL_2#KAPITTEL_2>

**Literature**

* 31 J. Marshall J. Info. Tech. & Privacy L. 145, "Eyes on the Road Program in Taiwan―Information Privacy issues under the Taiwan Personal Data Protection Act," 2015, <https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1758&context=jitpl>
* Leading Cases of the Taiwan Constitutional Court, "Background Note by the translator, No.631, Volume One, Judicial Yuan, 2018

**Other Sources**

* DataGuidance Taiwan - Data Protection Overview | Guidance Note | DataGuidance
* Freedom House, Taiwan Overview, <https://freedomhouse.org/country/taiwan/freedom-net/2021>
* Global Taiwan Institute, Closing Loopholes in the Legal Framework for Government Surveillance in Taiwan, Global Taiwan Brief, Vol. 5, Issue 3, 2020, <https://globaltaiwan.org/2020/02/closing-loopholes-in-the-legal-framework-for-government-surveillance-in-taiwan/>
* Legislative Yuan, <https://en.wikipedia.org/wiki/Legislative_Yuan>
* Lee and Li, Attorneys at Law, Newsletter, "The Telecommunications Management Act Becomes Effective on July 1, 2020," <https://www.leeandli.com/EN/NewslettersDetail/6496.htm>
* Taiwan Internet Transparency Report, Taiwan Association for Human Rights (TAHR), 2015, <https://transparency.tahr.org.tw/TITR_Report_2015_en.pdf>
* Google Transparency Report, Global requests for user information, Taiwan, <https://transparencyreport.google.com/user-data/overview?hl=en_US&user_requests_report_period=series:requests,accounts;authority:TW;time:&lu=legal_process_breakdown&legal_process_breakdown=expanded:0>

**Illustrations**

* OSI Model, <https://cdn.codegym.cc/images/article/3effcdd0-5b89-4574-b154-c2c1c65d945d/512.jpeg>

# Questions and Answers from Local Expertise at Nishimura & Asahi Taiwan Law Firm

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Question** | **Response (Yes or No)** | **Brief explanation (please include reference to source)** | **Likelihood of enforcement (Low Medium or High)** | **Further comments (if any)** |
| 1 | Is KS’ preliminary assessment of what Taiwanese legislation applies to the data transfer as set out above correct and complete?  If not, please describe any other laws or regulations that might apply to the data transfer. | No | * According to Paragraph 2, Article 51 of the PDPA, and the explanation promulgated by the competent authority (Fa-Lu-Zi No. 10403509750 dated 26 August 2015), **the PDPA applies to all collection, processing, and use of personal data occurring within the territory of Taiwan**, regardless of whether the data subject in question is located within Taiwan or not. * Furthermore, “processing” in the PDPA refers to the act of recording, inputting, **storing**, compiling/editing, correcting, duplicating, retrieving, deleting, outputting, connecting, or internally transferring data for the purpose of establishing or using a personal data file, and “use” refers to the act of **using personal data via any methods** other than processing. (Article 2 of the PDPA). * As such, in this case, through using GWE, Norwegian users’ personal data may be transferred and stored in data centres located in Taiwan and may be retransferred back to the EU/EEA from Taiwan. This constitutes processing and use of personal data within the territory of Taiwan, to which the PDPA shall apply. * In addition, Paragraph 2, Article 51 of the PDPA stipulates that the PDPA also applies where an entity collects, processes, or uses the personal data of Taiwan nationals outside the territory of Taiwan. It cannot be ruled out that such “entity” may include a foreign entity established or organised in any other country than Taiwan. Therefore, even if the processing occurs outside Taiwan, if the personal data processed through GWE includes data of Taiwan nationals (e.g., Taiwanese nationals residing in Norway), the PDPA may still apply. | High |  |
| 2 | Is there other general or sector-specific legislation that impacts data protection in the context of education or technology sectors, e.g. for datacenter, server and storage services for personal data? | - | * Apart from the legislations mentioned in the RFQ, regulations authorised by Article 27 of the PDPA oblige certain data holders to implement security measures to safeguard personal data. For example, according to “Regulations on the Personal Data Security Maintenance and Management in Digital Economy Related Industries” (數位經濟相關產業個人資料檔案安全維護管理辦法), which are applicable to data centres, servers, storage services, and relevant industries, managers of such facilities shall implement internal control protocol, among other security measures, to safeguard personal data (please refer to item 8 hereunder). * Articles 347 of the “Code of Civil Procedure” (民事訴訟法) stipulates that the court may order, by a ruling, a third person to submit documents and data in its possession. * Article 47 of the “Law Governing the Legislative Yuan’s Power” (立法院職權行使法), which came into force on 26 June 2024, provides that investigative committees assembled in the Legislative Yuan, which is the legislative body of Taiwan, may demand individuals or enterprises to provide documents and data related to their investigations. Data protection may be impacted in the highly unlikely event that Google is requested to submit or provide relevant data in accordance with above laws. | High  Low |  |
| 3 | Please consult our assessment of the CSSA above. Is our summary and assessment of the Act accurate based on the context provided by us and your understanding of the data that is stored in Taiwan and the GWE service? In particular, please advise of any independent control bodies. | No | * The CSSA governs communication surveillance conducted for the purposes of criminal investigation and national security. As it cannot be ruled out that Norwegian users of GWE may involve individuals or entities that fall into the definition of “foreign forces” in Article 8, or may be the subject of criminal investigation, the GWE service and relevant data is subject to the CSSA. * However, according to a precedent (最高法院106年度台非字第259號判決) of the Supreme Court of Taiwan, which has a de facto binding effect on courts, the CSSA applies to contents of **ongoing communications and data of communication records** (as defined in Paragraph 1 of Article 3-1, which means telecommunications numbers of the sender and the recipient, time of communication, length of use, address, service type, and mailbox or location information generated by the telecommunications system after the telecommunications user uses the telecommunications services) **and user information** (as defined in Paragraph 2 of Article 3-1, which means the telecommunications user’s name, identification document number, telecommunications number, and information in the application, for any type of telecommunications service), but not to other data. A search warrant issued in accordance with Article 122 and 128 of the Code of Criminal Procedure will be required to access other data stored in data centres. * Given its purposes of criminal investigation and national security, the competent authorities of the CSSA are courts, prosecutors’ offices, and the National Security Bureau. However, there is no independent control body specific to the CSSA. An independent data protection authority is being established in Taiwan (please refer to item 6 hereunder). * Since communication surveillance is of a covert nature, no immediate relief is provided in the CSSA, however, ex post remedy is available according to Article 19; court decisions are binding for national surveillance and intelligence services. | Low |  |
| 4 | Has the Telecommunications Management Act fully replaced the Telecommunications Act in Taiwan? | Yes | The TMA entered into force on 1 July 2020, and had a three-year transition period which ended on 30 June 2023. The TA remains in effect but serves only as the legal basis of certain statutory fee charges and has become irrelevant to data protection and other regulatory matters. The TMA has fully replaced the TA in this regard. | N/A |  |
| 5 | Does Google as a SaaS provider fall within the scope of Taiwanese telecom legislation?  Please elaborate on potential consequences for the data subjects' privacy rights. | Yes | It is correct that “telecommunications services” defined in the TA and TMA are limited to public communications services provided through the public switched telecommunications network (“PSTN”) and therefore Google as a SaaS provider does not fall within the scope of the TA and TMA. | N/A |  |
| 6 | Are any significant changes to applicable legislation expected?  If possible, please indicate when these changes will come into force. | - | * Regarding the PDPA, there is a significant legislative change expected as follows. * Currently, Taiwan does not have an independent data protection authority under the PDPA. Nevertheless, a recent amendment to the PDPA, dated 16 May 2023, designates the new Personal Data Protection Commission (“PDPC”) as the independent competent authority for personal data protection (Article 1-1 of the PDPA). Article 1-1 of the PDPA has not been enacted yet, as the PDPC has not been established at the present time. The preparatory office for the PDPC was established on 5 December 2023, and recent news reports suggest that the PDPC is expected to be established by August 2025. | N/A |  |
| 7 | Is a foreign data subject able to enforce their prescribed privacy rights in the jurisdiction under prescribed law, if relevant?  Please also indicate any perceived express hinderances in law, regulation or case law to such data privacy rights enforcement. | - | * In the event that a data subject, whether Taiwanese or foreign, has its personal data collected, processed, or used within the territory of Taiwan, the PDPA will apply. As such, the data subject may then enforce the privacy rights provided by the PDPA in that jurisdiction. * In addition, the prescribed privacy rights under the PDPA are as follows: (i) the right to make an inquiry regarding and to review his/her personal data; (ii) the right to request a copy of his/her personal data; (iii) the right to supplement or correct his/her personal data; (iv) the right to demand the cessation of the collection, processing, or use of his/her personal data; and (v) the right to erase his/her personal data. Article 3 of the PDPA also provides that such rights shall not be waived or limited contractually in advance, so there are no express hindrances to such data privacy rights enforcement under the PDPA. | N/A |  |
| 8 | Is there any security measures assumed to be effective for protection of data processed in Taiwan?  Please provide a brief overview of industry standards of data security provided in the region, if available. | - | * In reference to item 2 above, the “Regulations on the Personal Data Security Maintenance and Management in Digital Economy Related Industries” (數位經濟相關產業個人資料檔案安全維護管理辦法) require data centres, servers, storage services, and relevant industries to implement security measures to safeguard personal data files. The security measures provided therein are assumed to be effective for the protection of data processed in Taiwan. In addition, these regulations may apply to data centres located in Taiwan, including Google data centres storing Norwegian personal data in this regard. * These regulations provide an industry standard requiring data centres and relevant industries located in Taiwan to implement proper security measures to prevent personal data from being stolen, altered, damaged, destroyed, or disclosed as follows.  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. confirming restrictions on cross-border transfers, providing notice to data subjects, and supervising; 7. managing data security and personnel; 8. promoting awareness, education, and training; 9. managing facility security; 10. establishing an audit mechanism of data security; 11. keeping records, log files, and relevant evidence; and 12. implementing integrated and persistent improvements on the security and maintenance of personal data. | N/A |  |

1. <https://www.dataguidance.com/> [↑](#footnote-ref-2)
2. <https://transparency.tahr.org.tw/TITR_Report_2015_en.pdf> [↑](#footnote-ref-3)
3. <https://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021>, article 1 [↑](#footnote-ref-4)
4. <https://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021>, article 41, paragraph 2 [↑](#footnote-ref-5)
5. <https://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0050021> [↑](#footnote-ref-6)
6. For principles and rights, see articles 3, 5, 6, 8, 9, 10, 11, 18 and 19. [↑](#footnote-ref-7)
7. [Taiwan - Data Protection Overview | Guidance Note | DataGuidance](https://www.dataguidance.com/notes/taiwan-data-protection-overview), section 1.1, 3.1 [↑](#footnote-ref-8)
8. [Taiwan - Data Protection Overview | Guidance Note | DataGuidance](https://www.dataguidance.com/notes/taiwan-data-protection-overview), section 1.1 [↑](#footnote-ref-9)
9. Se note 5 [↑](#footnote-ref-10)
10. Se note 5 [↑](#footnote-ref-11)
11. See note 6, article 5 and 6. [↑](#footnote-ref-12)
12. <https://www.leeandli.com/EN/NewslettersDetail/6496.htm> and <https://freedomhouse.org/country/taiwan/freedom-net/2021> about how the TMA replaces the TA. [↑](#footnote-ref-13)
13. <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=K0060001>, Article 1. [↑](#footnote-ref-14)
14. See «Eyes on the Road Program in Taiwan―Information Privacy issues under the Taiwan Personal Data Protection Act, 31 J. Marshall J. Info. Tech. & Privacy L. 145» (2015), John Marshall Journal of Information Technology and Privacy Law is a review of the laws publish by a student organization at John Marshall Law School. The publications cover international information technology and privacy / data protection regulation. <https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1758&context=jitpl>, side 171. [↑](#footnote-ref-15)
15. <https://www.edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf> [↑](#footnote-ref-16)
16. European Essential Guarantees. <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf> [↑](#footnote-ref-17)
17. Ibid. [↑](#footnote-ref-18)
18. <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf>, section 26 – 31 [↑](#footnote-ref-19)
19. <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf>, section 26 [↑](#footnote-ref-20)
20. Ibid, section 28 [↑](#footnote-ref-21)
21. Ibid, section 29 [↑](#footnote-ref-22)
22. Ibid, section 30 [↑](#footnote-ref-23)
23. Ibid, section 31 [↑](#footnote-ref-24)
24. <https://en.wikipedia.org/wiki/Legislative_Yuan>. [↑](#footnote-ref-25)
25. [Taiwan - Data Protection Overview | Guidance Note | DataGuidance](https://www.dataguidance.com/notes/taiwan-data-protection-overview), section 1.1, 3.1. [↑](#footnote-ref-26)
26. <https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf>, section 46 and 47. [↑](#footnote-ref-27)
27. Taiwan – Third Country Assessment | Guidance Note | DataGuidance, section 2.3. [↑](#footnote-ref-28)
28. <https://www.dataguidance.com/notes/taiwan-data-protection-overview>, section 1.3. [↑](#footnote-ref-29)
29. <https://cons.judicial.gov.tw/en/docdata.aspx?fid=100&id=310812>, [↑](#footnote-ref-30)
30. Leading Cases of the Taiwan Constitutional Court, August 2018, Volume One, Judicial Yuan, No.631, «Background Note by the translator», pages 111 – 119. [↑](#footnote-ref-31)
31. <https://globaltaiwan.org/2020/02/closing-loopholes-in-the-legal-framework-for-government-surveillance-in-taiwan/> [↑](#footnote-ref-32)
32. Taiwan Internet Transparency Report, a research project on internet freedom and online privacy conducted investigate and track the personal data requests and content removal request situation done by government units, Taiwan Association for Human Rights (TAHR), <https://transparency.tahr.org.tw/TITR_Report_2015_en.pdf>. [↑](#footnote-ref-33)
33. Ibid, pages 10 – 11. [↑](#footnote-ref-34)
34. Ibid, page 27. [↑](#footnote-ref-35)
35. Taiwan Internet Transparency Report, a research project on internet freedom and online privacy conducted investigate and track the personal data requests and content removal request situation done by government units, Taiwan Association for Human Rights (TAHR), <https://transparency.tahr.org.tw/TITR_Report_2015_en.pdf>., page 26 [↑](#footnote-ref-36)
36. Ibid, page 25 [↑](#footnote-ref-37)
37. Ibid, page 24 [↑](#footnote-ref-38)
38. <https://transparencyreport.google.com/user-data/overview?hl=en_US&user_requests_report_period=series:requests,accounts;authority:TW;time:&lu=legal_process_breakdown&legal_process_breakdown=expanded:0> [↑](#footnote-ref-39)