# Reviews on Taiwan Constitutional Court's Judgment no. 13 of 2022


**Reviews on Taiwan Constitutional Court's Judgment no. 13 of 2022**

**2022/11/24**

**I.Introduction**

In 2012, the Taiwan Human Rights Promotion Association and other civil groups believe that the National Health Insurance Administration released the national health insurance database and other health insurance data for scholars to do research without consent, which may be unconstitutional and petitioned for constitutional interpretation.

Taiwan Human Rights Promotion Association believes that the state collects, processes, and utilizes personal data on a large scale with the "Personal Data Protection Law", but does not set up another law of conduct to control the exercise of state power, which has violated the principle of legal retention; the data is provided to third-party academic research for use, and the parties involved later Excessive restrictions on the right to withdraw go against the principle of proportionality.

The claimant criticized that depriving citizens of their prior consent and post-control rights to medical data is like forcing all citizens to unconditionally contribute data for use outside the purpose before they can use health insurance. The personal data law was originally established to "avoid the infringement of personality rights and promote the rational use of data", but in the insufficient and outdated design of the regulations, it cannot protect the privacy of citizens' information from infringement, and it is easy to open the door to the use of data for other purposes.

In addition, even if the health insurance data is de-identified, it is still "individual data" that can distinguish individuals, not "overall data." Health insurance data can be connected with other data of the Ministry of Health and Welfare, such as: physical and mental disability files, sexual assault notification files, etc., and you can also apply for bringing in external data or connecting with other agency data. Although Taiwan prohibits the export of original data, the risk of re-identification may also increase as the number of sources and types of data concatenated increases, as well as unspecified research purposes.

The constitutional court of Taiwan has made its judgment on the constitutionality of the personal data usage of National Health Insurance research database. The judgment, released on August 12, 2022, states that Article 6 of Personal Data Protection Act(PDPA), which asks *“data pertaining to a natural person's medical records, healthcare, genetics, sex life, physical examination and criminal records shall not be collected, processed or used unless where it is necessary for statistics gathering or academic research by a government agency or an academic institution for the purpose of healthcare, public health, or crime prevention, provided that such data, as processed by the data provider or as disclosed by the data collector, may not lead to the identification of a specific data subject”* does not violate Intelligible principle and Principle of proportionality. Therefore, PDPA does not invade people’s right to privacy and remains constitutional.

However, the judgment finds the absence of independent supervisory authority responsible for ensuring Taiwan institutions and bodies comply with data protection law, can be unconstitutional, putting personal data protection system on the borderline to failure. Accordingly, laws and regulations must be amended to protect people’s information privacy guaranteed by Article 22 of Constitution of the Republic of China (Taiwan).

In addition, the judgment also states it is unconstitutional that Articles 79 and 80 of National Health Insurance Law and other relevant laws lack clear provisions in terms of store, process, external transmission of Personal health insurance data held by Central Health Insurance Administration of the Ministry of Health and Welfare.

Finally, the Central Health Insurance Administration of the Ministry of Health and Welfare provides public agencies or academic research institutions with personal health insurance data for use outside the original purpose of collection. According to the overall observation of the

relevant regulations, there is no relevant provision that the parties can request to “opt-out”; within this scope, it violates the intention of Article 22 of the Constitution to protect people's right to information privacy.

**II.Independent supervisory authority**

According to Article 3 of Central Regulations and Standards Act, government agencies can be divided into independent agencies that can independently exercise their powers and operate autonomously, and non- independent agencies that must obey orders from their superiors. In Taiwan, the so-called "dedicated agency"(專責機關) does not fall into any type of agency defined by the Central Regulations and Standards Act. Dedicated agency should be interpreted as an agency that is responsible for a specific business and here is no other agency to share the business.

The European Union requires member states to set up independent regulatory agencies (refer to Articles 51 and 52 of General Data Protection Regulation (GDPR)). In General Data Protection Regulation and the adequacy reference guidelines, the specific requirements for personal data supervisory agencies are as follows: the country concerned should have one or more independent supervisory agencies; they should perform their duties completely independently and cannot seek or accept instructions; the supervisory agencies should have necessary and practicable powers, including the power of investigation; it should be considered whether its staff and budget can effectively assist its implementation. Therefore, in order to pass the EU's adequacy certification and implement the protection of people's privacy and information autonomy, major countries have set up independent supervisory agencies for personal data protection based on the GDPR standards.

According to this research, most countries have 5 to 10 commissioners that independently exercise their powers to supervise data exchange and personal data protection. In order to implement the powers and avoid unnecessary conflicts of interests among personnel, most of the commissioners are full-time professionals. Article 3 of Basic Code Governing Central Administrative Agencies Organizations defines independent agency as "A commission-type collegial organization that exercises its powers and functions independently without the supervision of other agencies, and operates autonomously unless otherwise stipulated." It is similar to Japan, South Korea, and the United States.

**III.Right to Opt-out**

The judgment pointed out that the parties still have the right to control afterwards the personal information that is allowed to be collected, processed and used without the consent of the parties or that meets certain requirements. Although Article 11 of PDPA provides for certain parties to exercise the right to control afterwards, it does not cover all situations in which personal data is used, such as: legally collecting, processing or using correct personal data, and its specific purpose has not disappeared, In the event that the time limit has not yet expired, so the information autonomy of the party cannot be fully protected, the subject, cause, procedure, effect, etc. of the request for suspension of use should be clearly stipulated in the revised law, and exceptions are not allowed.

The United Kingdom is of great reference. In 2017, after the British Information Commissioner's Office (ICO) determined that the data sharing agreement between Google's artificial intelligence DeepMind and the British National Health Service (NHS) violated the British data protection law, the British Department of Health and Social Care proposed National data opt-out Directive in May, 2018. British health and social care-related institutions may refer to the National Data Opt-out Operational Policy Guidance Document published by the National Health Service in October to plan the mechanism for exercising patient's opt-out right. The guidance document mainly explains the overall policy on the exercise of the right to opt-out, as well as the specific implementation of suggested practices, such as opt-out response measures, methods of exercising the opt-out right, etc.

National Data Opt-out Operational Policy Guidance Document also includes exceptions and restrictions on the right to opt-out. The Document stipulates that exceptions may limit the right to Opt-out, including: the sharing of patient data, if it is based on the consent of the parties (consent), the prevention and control of infectious diseases (communicable disease and risks to public health), major public interests (overriding) Public interest), statutory obligations, or cooperation with judicial investigations (information required by law or court order), health and social care-related institutions may exceptionally restrict the exercise of the patient's right to withdraw.

What needs to be distinguished from the situation in Taiwan is that when the UK first collected public information and entered it into the NHS database, there was already a law authorizing the NHS to search and use personal information of the public. The right to choose to enter or not for the first time; and after their personal data has entered the NHS database, the law gives the public the right to opt-out. Therefore, the UK has given the public two opportunities to choose through the enactment of special laws to protect public's right to information autonomy.

At present, the secondary use of data in the health insurance database does not have a complete legal basis in Taiwan. At the beginning, the data was automatically sent in without asking for everyone’s consent, and there was no way to withdraw when it was used for other purposes, therefore it was s unconstitutional. Hence, in addition to thinking about what kind of provisions to add to the PDPA as a condition for "exception and non-request for cessation of use", whether to formulate a special law on secondary use is also worthy of consideration by the Taiwan government.

**IV.De-identification**

According to the relevant regulations of PDPA, there is no definition of "de-identification", resulting in a conceptual gap in the connotation. In other words, what angle or standard should be used to judge that the processed data has reached the point where it is impossible to identify a specific person. In judicial practice, it has been pointed out that for "data recipients", if the data has been de-identified, the data will no longer be regulated by PDPA due to the loss of personal attributes, and it is even further believed that de-identification is not necessary.

However, the Judgment No. 13 of Constitutional Court, pointed out that through de-identification measures, ordinary people cannot identify a specific party without using additional information, which can be regarded as personal data of de-identification data. Therefore, the judge did not give an objective standard for de-identification, but believed that the purpose of data utilization and the risk of re-identification

should be measured on a case-by-case basis, and a strict review of the constitutional principle of proportionality should be carried out. So far, it should be considered that the interpretation of the de-identification standard has been roughly finalized.

**V.Conclusions**

The judge first explained that if personal information is processed, the type and nature of the data can still be objectively restored to indirectly identify the parties, no matter how simple or difficult the restoration process is, if the data is restored in a specific way, the parties can still be identified. personal information. Therefore, the independent control rights of the parties to such data are still protected by Article 22 of the Constitution.

Conversely, when the processed data objectively has no possibility to restore the identification of individuals, it loses the essence of personal data, and the parties concerned are no longer protected by Article 22 of the Constitution.

Based on this, the judge declared that according to Article 6, Item 1, Proviso, Clause 4 of the PDPA, the health insurance database has been processed so that the specific party cannot be identified, and it is used by public agencies or academic research institutions for medical and health purposes. Doing necessary statistical or academic research complies with the principles of legal clarity and proportionality, and does not violate the Constitution.

However, the judge believes that the current personal data law or other relevant regulations still lack an independent supervision mechanism for personal data protection, and the protection of personal information privacy is insufficient. In addition, important matters such as personal health insurance data can be stored, processed, and transmitted externally by the National Health Insurance Administration in a database; the subject, purpose, requirements, scope, and method of providing external use; and organizational and procedural supervision and protection mechanisms, etc. Articles 79 and 80 of the Health Insurance Law and other relevant laws lack clear provisions, so they are determined to be unconstitutional.

In the end, the judge found that the relevant laws and regulations lacked the provisions that the parties can request to stop using the data, whether it is the right of the parties to request to stop, or the procedures to be followed to stop the use, there is no relevant clear text, obviously the protection of information privacy is insufficient. Therefore, regarding unconstitutional issues, the Constitutional Court ordered the relevant agencies to amend the Health Insurance Law and related laws within 3 years, or formulate specific laws.

**Tsai, Yi-Jen**
**Project Manager**

**Release :** 2023/02