

Second Study Commission

Civil Law and Procedure

63rd Annual Meeting of the IAJ-San José (Costa Rica)

Questionnaire 2020

HOW DATA PROTECTION RULES

ARE IMPACTING ON CIVIL LITIGATION

In Nur-Sultan Kazakhstan we decided that in 2020, our Second Study Commission will focus on how data protection rules are impacting on civil litigation. We have limited the questionnaire to five questions and we expect to receive short but concise answers. The questions are as follows:

1. Do you store digital data in your jurisdiction?

In Taiwan, digital data may be stored in the form of microfilm or other electronic methods¹. Since 2019, our courts use electronic scanning equipment or other methods to convert the contents of paper documents which in case files into digital data to store in the form of electromagnetic records. Each court's electronic files can be exchanged, which promote the internal use of courts and the sharing of resources between courts, and enable electronic legalization of the production, acquisition, exchange, preservation, and management of documents².

2. How is it stored and for how long?

The storage and preservation of digital data is regulated by “The Implementation Regulations for Archives on Electronic Storage”. Permanent and temporary records shall be stored on separate electronic media. When processing the electronic storage of archives,

¹ Archives Act, article 9.

² Key points of the electronic operation of the court file, point 7.

the archivist shall comply with the regulations relevant to the regulatory mandates for government document and records management information system and apply proper electronic media and read-only storage format. Before processing electronic storage for paper records, they shall be organized first, and their fastener may be removed if necessary. If they are damaged, they shall be restored immediately. They shall be removed in order and be re-bound as originals after the completion of electronic storage. When processing electronic storage, one shall avoid distorting or skipping of pages of the records. Before processing electronic storage for photographic records, the preservation status of the photographs, microfilms, or films shall first be examined. If they are damaged, they shall be restored immediately. When processing the electronic storage of archives, the agency managing such archives shall check and ensure that the content shall be the same as on the original records. If necessary, they may be managed with electronic signature and stored with encryption.

The retention period for the following records shall be permanent³:

- (1) Those which relate to important systems, decisions or plans of the court holding the records.
- (2) Those which relate to enactments, amendments or interpretations of important laws or regulations of the court.
- (3) Those which relate to the organizational history or major activities of the court.
- (4) Those which have been of important value to national development or the administrative undertakings of the court.
- (5) Those of important value as evidence of the administrative undertakings of the court.

³ Regulations Governing the Retention Periods and Destruction of Agency Records, article 3.

- (6) Those of important value as evidence of important properties of the court.
- (7) Those which have exerted important influence on the protection of the interests of the court.
- (8) Those of important technological value.
- (9) Those of important historical, social, or cultural value.
- (10) Those pertaining to unusual matters that are materially newsworthy or are unique, special, or representative.
- (11) Those for which permanent retention is required by law.
- (12) Other records pertaining to important matters with permanent preservation value.

The retention period for temporary records shall be set at thirty years, twenty-five years, twenty years, fifteen years, ten years, five years or one year⁴. For a temporary record that has been converted to microfilm, electronic format, or some other format for the purpose of storage, the retention period for its original may be amended if the court has filed information showing that retention measures have been adopted which ensure that the reproduced and stored record can be effectively accessed⁵.

3. Who has access to the digital data in your jurisdiction?

Within the courts, judges and caseworkers involved in the cases are granted access. Those who are legally requested to read the file may pay and request the court to deliver the copy of the electronic file. A party may apply to the court clerk for inspection of, copying of, or

⁴ Regulations Governing the Retention Periods and Destruction of Agency Records, article 4.

⁵ Regulations Governing the Retention Periods and Destruction of Agency Records, article 7.

photographing the documents with expenses advanced.

Where a third party files the application, with the parties consent, or with a preliminary showing of his/her legal interests concerned, the court must decide the application.

Where the electronic file involve the privacy or business secret of the party or a third person and a grant of the application will likely result in substantial harm to such person, the court may, on motion or on its own initiative, render a ruling to deny the application or to restrict the application⁶.

4. Are there digital data protection rules in place in your jurisdiction?

The Personal Data Protection Act ("PDPA") is enacted on 11 August 1995 to regulate the collection, processing and use of personal data including digital data so as to prevent harm on personality rights, and to facilitate the proper use of personal data. 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 on any of the following bases⁷:

- (1) where it is expressly required by law.
- (2) where it is within the necessary scope for a government agency to perform its statutory duties or for a non-government agency to fulfill its statutory obligation, provided that proper security and maintenance measures are adopted prior or subsequent to such collection, processing or use of personal data.
- (3) where the personal data has been disclosed to the public by the data subject or has been made public lawfully.
- (4) where it is necessary for statistics gathering or academic research by a government agency or an academic institution for the purpose

⁶ Code of Civil Procedure, article 242.

⁷ Personal Data Protection Act, article 6.

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.

- (5) where it is necessary to assist a government agency in performing its statutory duties or a non-government agency in fulfilling its statutory obligations, provided that proper security and maintenance measures are adopted prior or subsequent to such collection, processing, or use of personal data.
- (6) where the data subject has consented to the collection, processing and use of his/her personal data in writing, except where the collection, processing or use exceeds the necessary scope of the specific purpose, or where the collection, processing or use based solely on the consent of the data subject is otherwise prohibited by law, or where such consent is not given by the data subject out of his/her free will.

5. Who covers the costs relating to the storage and protection of the digital data in your jurisdiction?

The budget of each court covers the cost relating to the storage and protection of digital information which it holds and is responsible for⁸.

⁸ Archives Act, article 4.