UNSW SYDNEY

UNSW Law & Justice Research Series

Mongolia's Unique Data Privacy Law Completes Coverage of Central Asia

Graham Greenleaf and Tamar Kaldani

[2022] *UNSWLRS* 52
(2022) 178 *Privacy Laws & Business International Report*, 25-28.

UNSW Law & Justice
UNSW Sydney NSW 2052 Australia

E: LAW-Research@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

Mongolia's unique data privacy law completes coverage of Central Asia

Graham Greenleaf and Tamar Kaldani

(2022) 178 *Privacy Laws & Business International Report*, 25-28.

The *Law of Mongolia on the Protection of Personal Information*, enacted in November 2021, and coming into force on 1 May 2022, marks the last country in Central Asia to enact a data privacy law.

Mongolia and its neighbours

Mongolia is a land-locked country situated between China and Russia, and its history has always been intertwined with those countries, and with the five other countries of Central Asia (Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, and Uzbekistan). It was considered to be an integral part of that history, particularly when the overland Silk Road was the only known route between Europe and China. Mongolia's history and culture diverged from the other Central Asian countries. Unlike five central Asian states, its predominant religion has been a version of Tibetan Buddhism since the 1700s and it was never part of the Russian Empire or the USSR. However, Mongolia was the first communist state to be formed after Russia and was ruled by a brutal dictatorship[1] from 1924 until its collapse (along with the Soviet Union) in 1990.

Since the 1990s Mongolia has undertaken what it describes as 'a transition to a market economy', as well as a peaceful transition to democratic government. Russian cultural influences still remain strong, in such matters as the use of the Cyrillic script for the Mongolian language, Russian being the second-most spoken language and many older members of the elite having been educated at Russian universities. Now English is gradually replacing Russian as the most common foreign language spoken in Mongolia, which is also seeking to strengthen partnerships beyond its immediate neighbours, wanting especially to advance in the fields of trade, education, energy and technology.[2] Mining of extensive mineral deposits, with exports to China, has joined traditional agriculture and herding as the basis of the Mongolian economy. With a population of under 3.5 million, it is the world's most sparsely-populated country.

International privacy commitments

Mongolia's 1992 Constitution provides that 'Privacy of citizens, their families, correspondence, and homes are protected by law',[3] and it also states that 'Mongolia fulfills in good faith its obligations under international treaties to which it is a Party.[4]

[1] Jasper Becker *The Lost Country* (Sphere, 1993) is a very readable history of Mongolia in the 20th century.

[2] The EU's Multiannual Indicative Programme 2021-2027 for Mongolia, page 4, https://international-partnerships.ec.europa.eu/system/files/2022-01/mip-2021-c2021-9051-mongolia-annex_en.pdf

[3] Article 13, Constitution of Mongolia < https://www.conscourt.gov.mn/?page_id=842&lang=en>

[4] Article 10 (2)

Mongolia is a party to the ICCPR, CRC and CRPD,[5] which include a commitment to protect privacy and the WTO (including GATS) relevant to data export limits). Otherwise, it is not a party to regional agreements involving data protection commitments, such as the APEC agreement or the various agreements between Russia and other Central Asian countries. If an international treaty to which Mongolia is a party provides otherwise than this Law, the provisions of the international treaty shall prevail (art 2.2).

In November 2017, the Partnership and Cooperation Agreement (PCA)[6] between the European Union and Mongolia entered into force, replacing a 1993 agreement, and an EU Delegation was established in Ulaanbaatar. One of its aims is to establish cooperation in data protection (art. 2(e)). It refers to agreement to protect personal data to the highest international standards, such as in the UN Guidelines for the Regulation of Computerized Personal Data Files,[7] and that such cooperation may include provision of technical assistance (art. 30). Although Mongolia's Law does indicate a considerable awareness of the EU's GDPR, the EU did not provide technical assistance in its development..

Scope and structure of the law

The Law applies generally to the processing of personal data by individuals, legal entities and non-legal entities, with no distinction between the public and private sectors. There is no indication of extra-territorial scope.

The Law does not apply (art. 3.3) to information about family members; the use of recording devices to protect a person's property or the life or health of a person or their family members; use of biometric information by a person to protect his or her property; and where information is subject to publication/disclosure in accordance with law' (see arts. 3.4-3.5). There are further partial exemptions from the Law, for collection, processing and use of information for the purpose of creating historical, scientific, artistic and literary works and preparing statistical information (art. 11); for journalistic purposes (art. 12); and for the collection, processing and use of genetic and biometric information, by specific government organisations or for specific purposes (art. 10).

Many terms are defined (art. 4), but of most significance is that 'personal information of a person' is defined broadly by specific inclusions and by the general inclusion of 'other information that may directly or indirectly identify or could identify a person'. The result is similar to the 'identifiability' test used in many other laws. Such a person is the 'information owner'. A data controller is defined as a person, legal entity or entity without legal status that collects, processes and uses information in accordance with the law or with the consent of the owner of the information.

'Sensitive information of a person' is defined to mean 'a person's nationality, race, ethnicity, religion, beliefs, health, correspondence, genetic and biometric information, digital signature private key, whether or not a person is serving a sentence, information concerning sexual and gender identity, expression, orientation and sexual life (art. 4.1.11). Such sensitive information is given protections additional to other personal information.

[5] List of UN treaties ratified by Mongolia https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=115&Lang=EN

[6] Partnership and Cooperation Agreement (PCA) http://data.consilium.europa.eu/doc/document/ST-9485-2015-ADD-1/en/pdf

[7] UN General Assembly Resolution 45/95 of 14 December 1990

The Law can therefore be described as 'largely comprehensive' in its scope.

The Law is composed of 8 chapters and 32 articles. It follows civil law structure and has no recitals to interpret the legal text. It also provides specific regulations concerning audio, video, and audio-visual recording systems (art. 27).

Information protection authorities

The Law divides the responsibilities of a data protection authority (DPA) between two organisations.

The National Human Rights Commission of Mongolia (NHRCM)[8] is given the following responsibilities (art. 24):

- To monitor the implementation of the Law, organise public awareness and advocacy activities, make submissions, and comment on regulations.
- To receive complaints and information concerning breaches of the Law, or act on its own initiative, to investigate, and to submit requirements and recommendations to the relevant authorities.
- To review the records submitted by the controllers regarding breaches and measures taken to eliminate negative consequences and make further recommendations where needed.
- To include information on these data protection activities in the reports made by the NHRC on human rights protection in Mongolia.
- To provide recommendations with regard to automated personal information processing systems, operating without continuous human supervision to prevent violations of human rights and freedoms (otherwise called 'automated decision-making' provisions).

One member of the NHRC shall be designated to fulfil functions under article 24. In effect, this member will be an 'Information Protection Commissioner'.

The Global Alliance of National Human Rights Institutions (GANHRI), which evaluates human rights bodies according to the Paris Principles, includes Mongolia's NHRCM as having 'A' status ('Fully compliant with the Paris Principles') as of 27 April 2022.[9] NHRCM's independence therefore has impartial verification.

The Ministry of Digital Development and Communications (MDDC) is given other responsibilities and powers, as the 'state central administrative body in charge of electronic development and communication on information protection in cyberspace' (as described in article 25). It is required:

- To ensure the implementation of the Law.
- To approve technological safety measures and procedures applicable to 'sensitive human information', and genetic and biometric information (all of which are defined).
- To receive and register information required to be provided by information offices as a result of data breaches, and 'take necessary measures immediately'.

[8] National Human Rights Commission (NHRCM) of Mongolia website https://en.nhrcm.gov.mn/; for history and functions, see < https://en.nhrcm.gov.mn/news/national-human-rights-commission-of-mongolia/>

[9] GANHRI 'Accreditation status as of 27 April 2022' <https://ganhri.org/wp-content/uploads/2022/04/StatusAccreditationChartNHRIs_27April2022.pdf >

The NHRCM and MDDC have already commenced meetings to coordinate their respective responsibilities.[10]

Obligations of data controllers

Collection and processing of personal information is generally treated as separate from use (including disclosure) of personal information.

A set of six general principles must be observed by all controllers: (i) not to violate human rights and freedoms; (ii) to respect human rights and legitimate interests; (iii) not to discriminate; (iv) to collect, process and use personal information on grounds provided by law, or with consent; (v) to ensure information security; and (vi) not to compromise accuracy and integrity (art. 5).

Controllers who are government organisations have separate grounds for legitimacy of collection, processing and use of personal information obligations (art. 6). The legitimate grounds for collection and processing by government organisations are: (i) consent of the information owner; as specified by laws; (ii) in the course of labour relations as provided by law; (iii) entry into and implementation of contracts; (iv) fulfilling Mongolia's treaty obligations; and (v) to exercise its functions without affecting legitimate interests of the information owner (art. 6.1).

For use of the information by government organisations, the legitimate grounds are: as specified by laws; to prevent harm to the information owner, or protect their legitimate interests; to prevent harm to the legitimate interests of others; and to create historical, scientific, artistic and literary works, and anonymised statistical information (art. 6.2). An anonymisation procedure is specified.

Collection, processing and use by non-government controllers have different legitimate grounds (art. 7): the first four grounds under article 6.1; disclosure to the public in accordance with law; and the final ground in article 6.2 (creating works and statistics).

The same obligations concerning permission (consent) – and to subsequent use or transfer – apply to all controllers (art. 8). Related obligations arise from article 18 (shown in parentheses), which must be read with article 8.

- Consent of the information owner must be obtained, except as provided by law. (Identification such as an ID card must be obtained.)
- Notice to the information owner of proposed conditions of use must be given. (including explanations of purpose and grounds for collection, and the right to refuse consent and consequences of doing so).
- Consent must be written, on paper or in electronic form – as provided by law or accepted by the information owner.
- Consent must be by a positive act.
- Consent may be revoked at any time.
- The controller has the onus to prove consent.

[10] NHRCM website News 'There to be cooperation on the law on protection of personal data and other relevant draft laws and regulations' < https://en.nhrcm.gov.mn/news/there-be-cooperation-law-protection-personal-data-and-other-relevant-draft-laws-and-regulations/ >

- Consent must be obtained again if the controller proposes to use the personal information for a purpose other than the purpose for which consent was originally obtained.
- Similarly, consent to transfer the information must be obtained unless the details of the transfer were provided by notice when the information was originally collected. The same rules apply to such consent as apply to consent for secondary uses.

Other obligations included in article 18 cover such matters as the duty to keep records of processing; duty to approve and enforce internal procedures for data collection, processing and use; to make corrections as requested by the information owner; to receive and resolve complaints by information owners and to inform him/her about the deployment of automated personal information processing systems and its consequences.

The law provides an exhaustive list of the grounds for the deletion of personal information. Namely, the information should be deleted (art. 15): upon the request of the information owner if the information has been processed contrary to the Law; because laws, treaties or court decisions so require; the original purpose of collection as defined by law, contract or other agreement with information owner has been achieved; or any other grounds specified by the law. Otherwise, personal information may not be deleted.

Sensitive information (art. 9) should be kept confidential, and its collection, processing and use is prohibited unless (i) there are legal grounds provided for by articles 6 and 7 of the law, (ii) processing is necessary for the protection of the health of information owner or others and provision of medical services by health professional subject to the conditions and obligations specified by law, (iii) processing is necessary for providing explanations, statements and evidence related to legal claims in accordance with the law. The conditions under which government organisation can make use of genetic and biometric information are very specific and restrictive (art. 10).

Export of personal data overseas is prohibited unless with the consent of the information owner, or as provided by law (otherwise unspecified), or in accordance with a treaty to which Mongolia is a party (art. 14). Unlike the GDPR, Mongolia's law has not adopted an adequacy decision mechanism or attribured any role to DPAs concerning international data transfers.

The obligations of processors who are in a contractual relationship with the controller are separately set out (art. 19).

Information security requirements are to be determined by the MDDC (art. 20.2), through regulations. Where there is what is generally referred to as a 'data breach', information processors are required to notify the controllers, and to inform the information owner if their interests are harmed (art. 22). However, there is no explicit requirement that the controller should immediately inform the MDDC or the NHRCM, which is the normal 'data breach notification' requirement. The NHRCM only needs to be notified of the details in January each year or at the request of NHRCM (art. 22.6).

The use of automated personal information processing systems, operating without continuous human supervision, is allowed but requires an 'assessment' of their operation to be made wherever they (i) make decisions affecting the rights, freedoms and legitimate interests of information owners; or (ii) regularly process sensitive human information. The methodology for such an assessment is to be approved by the MDDC, based on the proposal of the NHRCM, and the data collected by the assessment is to be submitted to the NHRCM by the controllers.

The obligations described above cover most of the obligations of data controllers in the GDPR, but some are not found, including the following: data protection by design and by default; demonstrable accountability by controllers; mandatory Data Protection Impact Assessments (DPIAs) for likely high risk processing; mandatory Data Protection Officers (DPOs) for sensitive processing. Other obligations such as data breach notification are only implemented in an incomplete form.

Rights of information owners

Information owners have an extensive set of rights (art. 16.1):

- to give consent to collection, on a voluntary basis;
- to know of collection, processing or use;
- to know the information required to be given as notice during collection;
- to know of transfers to third parties;
- to notify the controller if the personal information is erroneous or incomplete;
- to notify the controller when the destruction of information is required;
- to demand collection or destruction of information when required by law;
- to obtain a copy (paper or electronic) of the information;
- to have this copy transmitted to a third party ('data portability'), to be done without violating the rights of others (art. 17.1.3);
- to request blocking of processing;
- to file a complaint, or express an opinion on a decision made as a result of processing, provide additional information and demand re-consideration.

These rights extend to deceased persons, on whom personal information can only be collected, processed or used with the written consent of the testator, their family member or legal representative, unless otherwise allowed by law. This restriction lasts 70 years after death (art. 13).

Mongolia's law does require the protection of almost all the rights of data subjects provided for in the EU's GDPR, although the wording is sometimes ambiguous. Some of these 'GDPR rights' which are not provided, or at least not clearly stated, include: some aspects of stronger requirements for consent; representative actions by NGOs on behalf of information owners (GDPR art. 80); and the 'right to be forgotten'.

Enforcement

The enforcement aspects of the law are stated in very general terms and rely upon interaction with other Mongolian laws for the substance to be determined.

Information owners can submit complaints against state organisations in accordance with the General Administrative Law and related laws. Complaints against private sector organisations can be submitted for resolution either to 'the competent authority' or to the NHRCM. If the information owner does not agree with the decision made by any of these bodies, there is a right of appeal to the courts (art. 28).

Information owners are entitled to protection (such as injunctions), and to compensation for illegal damage to their rights, including for non-pecuniary damage (art. 16.2).

Violations of the Law can also be enforced without need for a complaint. Violations by officials will be dealt with by the Criminal Law, the Civil Service Law, or the Labour Law, as

appropriate. Violations by persons or legal entities who are not officials will be subject to liability specified in the Criminal Code or the Law on Violations (art. 30).

Some specific acts are also prohibited. Processing of information for purposes other than those specified in the law, or for which permission was originally obtained is prohibited (art. 29.1). Processing personal information without human intervention is also prohibited, if it results in a violation of rights and freedoms (art. 29.2).

Comparison with the GDPR is complex, because of the need to consider other Mongolian laws. Even though the law is not explicit concerning penalties, amendments to the Criminal Code and Law on Offence have been proposed, providing specific criminal and administrative sanctions, including financial fine up to MNT 20,000,000 (around 6300 Euros) for legal entities.[11]

Conclusions: Unique in its region

Mongolia's law provides stronger data protection that any of the other five Central Asian countries. At least on paper, it is a stronger law than is found in almost any of the 26 countries in Asia from Japan to Afghanistan, provided we assume that the enforcement aspects will be effective and dissuasive of breaches.

In comparison with the GDPR, Mongolia's law is a reasonably strong in implementation of its principles. It is relatively comprehensive, and it involves an independent supervisory body (uncommon in Asia), but the strength of its enforcement provisions waits to be seen. As is listed above, the Law includes most of the GDPR obligations on controllers and processors, and most of the rights of data subjects. The laws of China, Russia or the other five Central Asian countries, have had no obvious influence on Mongolia's law in such areas as registration obligations for controllers, or data localisation requirements. These countries have no equivalent to Mongolia's independent Human Rights Commission involved in their laws. Mongolia's data privacy law should prove to be relatively friendly to both Mongolian data subjects and to foreign businesses in Mongolia.

In the context of Central Asia and its neighbours, Mongolia's law is at least unusual, perhaps unique, in some aspects of its structure and its terminology, and in its approach to enforcement, but in its substance it is quite a conventional data privacy law, and one which is more up-to-date than most other laws outside Europe.

[11] DLA Piper website at <https://www.dlapiperdataprotection.com/index.html?t=enforcement&c=MN>