

(2022.07.08-ны өдрийн орчуулга) Unofficial translation

LAW OF MONGOLIA

December 17, 2021

Ulaanbaatar city

ON Personal Data Protection

(Revised edition)

CHAPTER one

general provision

Article 1. Purpose of the Law

1.1. The purpose of the Law is to regulate relations with respect to the collection, processing, use and security of personal data.

Article 2. Legislation on Personal Data Protection

2.1. Legislation on the personal data protection shall consist of the Constitution of Mongolia, Civil Code, Law on Transparency of Public Information, this Law, and other legislative acts enacted in conformity therewith.

2.2. If an international treaty to which Mongolia is a party provides other than this law, the provisions of the international treaty shall prevail.

Article 3. Scope of the Law

3.1. This law shall regulate the relations with respect to the collection, processing, use and security of personal data ("data") by a person, legal entity, or non-legal entity.

3.2. This law shall also equally apply to relations with respect to the data collection, processing, use and security with the assistance of hardware and software.

3.3. The law shall not apply to the following relations:

3.3.1. Collection, processing, use and security of data regarding oneself or one's family members without violating the right to liberty and security of such person.

3.3.2. Installation of audio, video and audio-video recording devices for the protection of movable and immovable property owned, possessed, and used as well as oneself or one's family members life and health .

3.3.3. Use of one's biometric data for the protection of movable and immovable property owned, possessed, and used, and storage of its data.

3.3.4. Disclosure of information as provided under the law.

3.4. The Law shall regulate the relations with respect to personal secrets other than those specifically regulated by the Law on Intelligence Activity.

3.5. This Law shall regulate relations other than those specified in the Law on Crime and Offense Prevention with respect to the installation of video recorders in publicly possessed streets, areas, squares, and public places in order to prevent from crime and offence or for ensuring the traffic safety.

Article 4. Definitions of Terms of the Law

4.1. The following terms specified in this law shall have the following meanings:

4.1.1. "Biometric data" means non-overlapping physiological data related to the human body such as fingerprints, iris, face, voice, and gait which can be identified with equipment, technical tool, and software.

4.1.2. "Genetic data" means unique information indicating a person's physiological, health and hereditary characteristics determined by the analysis of a biological sample.

4.1.3. "Immediately" means the shortest possible duration.

4.1.4. "Correspondence data" refers to the information exchanged using letters, parcels, emails, communications, and information technology.

4.1.5. "Data subject" refers to a person identified by the information provided in Sub-paragraph 4.1.11 of this Law or legal representative of a citizen provided in Articles 17, 18 and 19 of the Civil Code, or of a citizen stated in the Article 16 of such code, unless otherwise provided by law.

4.1.6. "Data use" refers to Sub-paragraph 4.1.4 of the Law on Transparency of Public Information.

4.1.7. "Data processing" refers to Sub-paragraph 4.1.5 of the Law on Transparency of Public Information.

4.1.8. "Data controller" refers to a person, legal entity or non-legal entity which collects, processes, and uses data in accordance with the law or with the consent of the data subject.

4.1.9. "Data collection" refers to Sub-paragraph 4.1.6 of the Law on Transparency of Public Information.

4.1.10. "Property information" means information on the property owned, possessed, and used by the data subject.

4.1.11. "Personal data" means sensitive personal data and other information which can directly or indirectly identify or potentially identify a person, including parents' name, first name, date of birth, place of birth, place of residence, address, location, citizen's registration number, property, education, membership, and electronic identifiers.

4.1.12. "Sensitive information" means information in regards with a person's race, ethnic origin, religion, beliefs, health, correspondence, genetic and biometric data, digital signature private key, criminal records, sexual and gender orientation, expression, and sexual relations.

4.1.13. "Deidentification" refers to the prevention of linking information or data to a person.

4.1.14. "Electronic identifier" means login name to access any information system, email address, social media account, wired and wireless technology addresses, and information on other types of equipment and information system.

4.1.15. "Data concerning health" means information related to the physical or mental health and provision of healthcare services.

Article 5. Principles for Data Collection, Processing, and Use

5.1. Data collection, processing and use shall comply with following principles:

5.1.1. Refrain from violating human rights and freedom.

5.1.2. Respect human rights and legitimate interests.

5.1.3. Refrain from discrimination.

5.1.4. Collect, process and use data based on grounds specified in laws or with the consent of the data subject.

5.1.5. Ensure data security.

5.1.6. Ensure data accuracy and integrity.

Chapter two

Data collection, processing and use

Article 6. Data Collection, Processing and Use of State Authorities

6.1. The state authority shall collect and process data on the following grounds:

6.1.1. With the consent of the data subject.

6.1.2. On the grounds specified by law.

6.1.3. Data controller to exercise the rights and fulfil the obligations in employment relations in cases provided by law.

6.1.4. Execute contracts and ensure the implementation of executed contracts.

6.1.5. Comply with obligations under international treaties to which Mongolia is a party.

6.1.6. Implement its legal functions without affecting the rights and legitimate interests of the data subject.

6.2. The state authority shall use data on the following grounds:

6.2.1. With the consents of the data subject.

6.2.2. On the grounds specified by law.

6.2.3. Prevent damage and harm to the life, body, rights, freedom, and property of the data subject, and protect its rights and legitimate interests.

6.2.4. Prevent damage and harm to the rights and legitimate interest of others.

6.2.5. Create historical, scientific, artistic, literary works and prepare statistical information by de-identifying a person.

6.3. The state authority shall follow the procedure set forth in Article 12 of the Law on Transparency of Public Information for the de-identification of the data subject in order to make the information available to the public.

Article 7. Data Collection, Processing and Use by Person, Legal Entities and Non-Legal Entities

7.1. Individuals/person, legal entities, and non-legal entities other than state authorities shall collect, process, and use data on the following grounds:

7.1.1. On grounds specified in Sub-paragraphs 6.1.1, 6.1.2, 6.1.3, and 6.1.4 of this Law.

7.1.2. Disclosed to the public as specified in the Law.

7.1.3. Create historical, scientific, artistic, literary works and prepare statistical information by de-identifying a person.

Article 8. Consent from Data Subject

8.1. The data controller shall seek a consent from the data subject for data processing, collection, and use, except as provided by law.

8.2. The data controller, in order to obtain a consent, shall introduce the following conditions to the data subject, including:

8.2.1. Clear and specific grounds and purposes for data collection, processing, and use.

8.2.2. Data controller's name or a legal entity's given name and contact information.

8.2.3. List of data required for collection, processing, and use.

8.2.4. Duration of data processing and use.

8.2.5. Information on whether the data will be made available to the public.

8.2.6. Information on whether the data will be transferred to others, and if so, the list of information to be transferred.

8.2.7. Form of withdrawal of consent.

8.3. The data subject shall give a written consent to the data controller, which shall be in paper or electronic form.

8.4. The consent in electronic form specified in Paragraph 8.3 of this Law shall be granted by identifying and certifying in an electronic environment by means specified in the law or accepted by the data subject.

8.5. The consent shall be sought from a legal representative for collection of data of a citizen provided in Articles 17, 18 and 19 of the Civil code, or of a citizen stated in Article 16 of such code, unless otherwise provided by law.

8.6. The data subject's failure to respond to the data collection consent and the expiration of response timeframe or the expiration of a reasonable time frame, shall not become grounds for deeming the data collection is permitted.

8.7. The data subject may withdraw the consent at any time and the data processed prior to the receipt of the request for withdrawal shall remain lawful if it does not violate this law.

8.8. The consent of the data subject shall not be required for data collection for the purpose of identifying affiliated parties specified in Sub-paragraph 4.1.6 of the Law on Competition of the participants/bidders in the procurement of goods, works and services with state and local funds.

8.9. The data controller shall prove that the consent of the data subject has been acquired for data collection.

8.10. The data controller shall request a consent from the data subject again if the data will be processed or used for a purpose other than those for which a consent was originally provided.

8.11. Unless a consent was provided as specified in Sub-paragraph 8.2.6 of this Law, the data controller shall seek a consent in the form specified in Paragraph 8.3 of this Law from the data subject for data transfer.

8.12. The regulations specified in Paragraphs 8.4, 8.5, 8.6, 8.7 and 8.9 of this Law shall equally apply to seeking a consent to data transfer.

Article 9. Collection, Processing and Use of Sensitive Personal Data

9.1. Sensitive data on health, correspondence, genetic and biometric data, digital signature private key, sexual and gender orientation, expression, and sexual relations specified in Sub-paragraph 4.1.12 of this Law shall be considered as personal secrets.

9.2. Collection, processing or use of sensitive personal data shall be prohibited except in the

following cases:

9.2.1. Provided in Articles 6 and 7 of this Law.

9.2.2. Healthcare staff to exercise their rights and fulfill obligations specified in the law for the protection of the health of the respective person or others and provision of healthcare services.

9.2.3. Provide an explanation, statement, and evidence in accordance with the law for the requirements of the claims from citizens and legal entities.

9.3. The National Human Rights Commission of Mongolia ("National Human Rights Commission") may make recommendations to data controllers in order to prevent violations of human rights and freedoms in the collection, processing and use of sensitive personal data.

Article 10. Collection, Processing and Use of Genetic and Biometric Data

10.1. The following state authorities shall collect and use human genetic and biometric data, in accordance with the grounds and procedures provided by law, for following purposes:

10.1.1. Non-overlapping physiological data (fingerprints) by the state registration authority for the purpose of maintaining civil state registration and monitoring registration of voters.

10.1.2. Biometric data by border protection authority for the purpose of identifying and verifying a foreign citizen crossing the state border.

10.1.3. Genetic and biometric data by the competent authority specified in the law for the purpose of combating, preventing, and investigating crimes and offences.

10.1.4. Genetic and biometric data by a forensic organization for forensic analysis conducted during the course of resolving a case or dispute.

10.1.5. Biometric data of a member of the State Great Khural for the purpose of registering for the meeting and voting.

10.2. An employer may use biometric data other than non-overlapping physiological data (fingerprints) with the employees' consent in order to facilitate the identification and verification of employees under the internal labor procedures.

10.3. An employer is prohibited to process, change or transfer data used as per Paragraph 10.2 of this Law to other persons.

10.4. The data controller shall ensure the security of the collection and use of genetic and biometric data.

10.5. The data controller's compliance with the information security requirements established under the procedure set forth in Sub-paragraph 25.1.2 of this Law shall not serve as a ground for exemption from liability for information loss.

Article 11. Data Collection, Processing and Use for Historical, Scientific, Artistic and Literary and Statistical Purposes

11.1. Unless otherwise provided by law, data shall be collected with the consent of the data subject for the purpose of creating historical, scientific, artistic, and literary works and preparing statistical information.

11.2. The data may be processed and used for the purpose of creating historical, scientific, artistic, and literary works and preparing statistical information, regardless of the purpose of the data collected.

11.3. Unless otherwise provided by law or with the written consent of the data subject, the data may be processed and used through de-identification for the purpose of creating historical, scientific,

artistic, and literary works and preparing statistical information.

11.4. The rights and legitimate interests of the data subject and others may not be violated in creating historical, scientific, artistic, and literary works and preparing statistical information.

11.5. Sub-paragraphs 16.1.1, 16.1.2 and 16.1.3 of this Law shall not apply to the data subject for processing and using data for the purposes specified in Paragraph 11.1 of this Law.

11.6. Security measures shall be taken in accordance with Article 20 of this Law for processing and using data for the purpose of creating historical, scientific, artistic and literary works and preparing statistical information.

Article 12. Data Collection, Processing and Use for Journalistic Purposes

12.1. Data may be collected, processed, and used for journalistic purposes or protecting public interests.

12.2. It is prohibited to collect, process, and use data regarding health, correspondence, genetic and biometric data, sexual and gender orientation, expression, and sexual relations for the purposes specified in Paragraph 12.1 of this Law without the consent of the data subject.

12.3. The rights and legitimate interests of the data subject and others may not be violated during the data collection, processing and use for journalistic purposes.

Article 13. Data Collection, Processing and Use Following the Death of the Data Subject

13.1. Unless otherwise provided by law, if the data subject is deceased or is considered to be deceased, the relevant data shall be collected, processed, and used based on the will or the written consent of his or her family member, or legal representative.

13.2. Unless otherwise provided by law, if 70 years passed since the death of the data subject, a consent is not required for the collection, processing or use of sensitive information.

Article 14. Data Transfer to Foreign Individuals, Legal Entities, and International Organizations

14.1. Data transfer to foreign individuals, legal entities, or international organizations is prohibited, except as provided in laws, international treaties which Mongolia is a party, or with the consent of the data subject.

Article 15. Data Erasure

15.1. Data controller shall erase the data on the following grounds:

15.1.1. By the request of the data subject, if the data has not been collected, processed, or used in accordance with the grounds and procedures provided by the law.

15.1.2. Data controller's obligation to erase the data under the laws, international treaties to which Mongolia is a party, and legally enforceable court decisions.

15.1.3. Data other than collected and processed under the law has achieved the purpose for which it was originally collected or has been specified in the contract or has been mutually agreed upon.

15.1.4. Other grounds, as provided by law.

15.2. Unless otherwise provided by law, data erasure shall be prohibited except for the grounds specified in Paragraph 15.1 of this Law.

Chapter three

Data subject's rights and obligations

Article 16. Data Subject's Rights

16.1. The data subject shall have following rights:

16.1.1. Give or refuse to give a consent to the data controller for data collection on a voluntary basis.

16.1.2. Know whether his or her data has been collected, processed, and used.

16.1.3. Know about the information provided in Paragraph 8.2 of this Law.

16.1.4. Know about the third party who has received or is going to receive the data regarding the data subject to the third party.

16.1.5. Notify the data controller to rectify inaccurate data, make changes, and provide additional data.

16.1.6. Notify the data controller of the data erasure under the law for data erasure.

16.1.7. Demand the erasure of the data if the law prohibits data collection and provides for erasure.

16.1.8. Obtain a copy of the relevant information from the data controller in paper or electronic form.

16.1.9. Transfer a copy of the data specified in Sub-paragraph 16.1.8 of this Law to the selected data controller.

16.1.10. Request cancellation in the course of data collection, processing, and use, and to notify the data controller in writing.

16.1.11. File a complaint or provide an explanation on the decision made as a result of data processing, provide additional data and demand data processing again.

16.2. If the data subject considers that his or her rights and freedoms specified in this law and international treaties of Mongolia have been violated, he or she shall have the right protected and illegal damage and non-pecuniary damage rectified.

Article 17. Data Subject's Obligations

17.1. The data subject has following obligations:

17.1.1. Ensure the accuracy and security of the relevant data.

17.1.2. Notify the data controller to rectify inaccurate data, make changes, and provide additional data.

17.1.3. Avoid violating the rights and freedoms of others and affecting their legitimate interests while exercising the rights specified in Sub-paragraph 16.1.9 of this Law.

Chapter four data controller and data processor

Article 18. Data Controller

18.1. The data controller shall collect, process, and use data based on the grounds specified in the law or with the consent of the data subject.

18.2. The data controller shall have the following responsibilities regarding the data collection, processing and use:

18.2.1. Approve and enforce procedures for data collection, processing and use under the Law.

18.2.2. Seek a consent from a data subject for data collection in accordance with Paragraph 8.4 of this Law or on the basis of identifying and verifying the data subject with ID card or similar document.

18.2.3. Provide the information specified in Paragraph 8.2 of this Law in order to seek a consent from the data subject, provide clear explanation on the purpose and grounds for data collection.

18.2.4. Explain the data subject about the right for refusal to give a consent for data collection and filing a complaint related to the data collection, processing, and use.

18.2.5. Explain the consequences that may arise if the data subject refuses to give a consent for data collection.

18.2.6. Explain the data subject about the decision-making based on electronic data processing without any human involvement and consequences of such decisions.

18.2.7. Verify the data against with the original copy of the data subject's ID card or similar document, or the information delivered electronically or placed in the database.

18.2.8. Provide information on data processing and use at the request of the data subject.

18.2.9. Rectify, change, erase data at the request of the data subject and notify the data subject accordingly.

18.2.10. Terminate the data processing and use after receiving the data subject's request unless the rights and legitimate interests of others are affected.

18.2.11. Provide a copy of the data in electronic form free of charge at the request of the data subject.

18.2.12. Keep records on data collection, processing, and use

18.2.13. Store information obtained in the course of data collection, processing, and use.

18.2.14. Receive and resolve the complaint of the data subject and provide a response.

18.2.15. Accept liability before the data subject on the data collection, processing and use, or before to the authorized organizations and third parties in cases provided by law.

18.3. The conditions for termination of the data processing and use specified in Sub-paragraph 18.2.10 of this Law shall not apply to the cancellation of the processing and use of data related to the data subject.

18.4. The data controller shall revoke the consent at the request of the data subject in an easy and understandable manner without causing any inconvenience.

Article 19. Data Collection and Processing on a Contractual Basis

19.1. The data controller may transfer the obligation for data collection and processing to the data processor on a contractual basis.

19.2. The contract specified in Paragraph 19.1 of this Law shall include the purpose of data collection and processing, the term of the contract, the data list and the conditions for protecting the rights of the data subject.

19.3. Unless otherwise provided in the contract specified in Paragraph 19.1 of this Law, the data processor shall be prohibited from transferring his or her obligations to the others and the liabilities shall be clearly stated in the contract.

19.4. The data processor who has taken over the responsibility of data collection and processing shall have the following responsibilities, including:

19.4.1. Collect and process data under the supervision of the data controller with the consent from the data subject.

19.4.2. Rectify, change, or erase data in accordance with the duties, directions and instructions given by the data controller

19.4.3. Provide the data controller the necessary information related to data collection and processing.

19.4.4. Maintain data obtained in the course of data collection and processing.

19.4.5. Provide information and results of data processing to the data controller within the period specified in the contract without keeping a copy, and erase the data which was collected for processing without re-use.

19.4.6. Take measures to ensure information security in accordance with Article 20 of this Law.

19.4.7. Perform the duties, directions and instructions given by the data controller within the procedure specified in 18.2.1 of this Law.

19.5. The data processor's violation of the duties, directions and instructions given by the data controller shall not serve as a ground to release the data controller from the obligations and responsibilities to the data subject.

CHAPTER FIVE INFORMATION PROTECTION

Article 20. Information Security Measures

20.1. The data controller and data processor specified in Paragraph 19.1 of this Law, for information security, shall take the following measures:

20.1.1. Approve and follow internal procedures to ensure information security in accordance with the requirements set forth in Paragraph 20.2 of this Law.

20.1.2. Approve a plan for taking actions for loss of information and notifying the data subject and relevant state authority in accordance with the Law.

20.1.3. Take all measures to ensure the integrity, confidentiality and accessibility of the information system used for data collection, processing, and use.

20.1.4. Approve and follow procedures and guidelines on data use restriction, data erasure and deidentification of data subject.

20.1.5. Conduct an assessment in order to ensure the security of data processing activities.

20.2. The state central administrative body in charge of digital development and communication shall determine the requirements for ensuring information security during data collection, processing and use, instructions for assessment and storage technology requirements.

Article 21. Notice to Data Subjects

21.1. The data controller shall immediately provide a notice to the data subject in the following cases:

21.1.1. Use of sensitive personal data.

21.1.2. Data processed for grounds and purposes other than processing data with the consent of data subject and transfer of such processed data to third parties.

21.1.3. Change of conditions specified in Paragraph 8.2 of this Law following the collection of the data from the data subject.

21.2. The data controller may submit a notice for the collection, processing and use of the information of the data subject, except for the cases specified in Paragraph 21.1 of this Law.

Article 22. Notification of Violations in the Data Collection, Processing and Use

22.1. The data processor specified in Paragraph 19.1 of this Law shall immediately notify the data controller of any violations identified during data collection and processing.

22.2. If the violation specified in Paragraph 22.1 of this Law harms the rights and legitimate interests of the data subject, the data controller shall immediately notify the data subject.

22.3. The notice specified in Paragraph 22.2 of this Law shall contain the following:

22.3.1. Data subject and data records related to the violation.

22.3.2. Name and contact information of the data subject

22.3.3. Violation and possible negative consequences.

22.3.4. Responses to eliminate the violation and potential negative consequences.

22.4. The data subject shall have the right to file a complaint to the relevant authority in accordance with the law if he or she considers that his or her rights and legitimate interests have been harmed due to the violation specified in Paragraph 22.2 of this Law.

22.5. The data controller shall keep a record of the response taken to eliminate the violation and its negative consequences.

22.6. The record specified in Paragraph 22.5 of this Law shall be submitted to the National Human Rights Commission in January of each year or as requested.

Article 23. Assessment

23.1. The data controller may use electronic data processing technology for data collection, processing, and use without any human involvement, and an assessment shall be completed in following cases:

23.1.1. Decision-making which could potentially affect the rights, freedoms, and legitimate interests of the data subject.

23.1.2. Regular processing of sensitive personal data.

23.2. Data shall be collected, processed and used using electronic data processing technology based on the recommendations of the National Human Rights Commission provided for the assessment specified in Paragraph 23.1 of this Law.

23.3. The state central administrative body in charge of digital development and communication shall approve the methodology and procedure for conducting the assessment specified in Paragraph 23.1 of this Law based on the proposal of the National Human Rights Commission.

Chapter six data protection authority

Article 24. Full Power of the National Human Rights Commission for Information Protection:

24.1. The National Human Rights Commission shall exercise the following full powers with

respect to information protection:

24.1.1. Monitor the compliance of the laws on personal data protection, raise public awareness and organize advocacy activities, submit requirements and recommendations to relevant organizations, and comment on relevant procedures.

24.1.2. Receive, investigate, and resolve complaints and reports, if it is considered that human rights and freedoms protected by this Law have been violated or potentially violated in the course of the data collection, processing, use and protection or investigate and resolve on its own initiative and submit requirements and recommendations to the relevant authorities on the respective matter.

24.1.3. Provide directions and recommendations to relevant organizations regarding collection, processing, use and protection of personal sensitive data.

24.1.4. Receive and review reports submitted by the data controller on violations identified in the data collection, processing and use and measures taken to eliminate its negative consequences and make recommendations on further considerations.

24.1.5. Make recommendations for the purpose of preventing violations of human rights and freedoms in the data collection, processing and use with electronic processing technology in accordance with Article 23 of this Law.

24.1.6. Specify data protection activities, violations, and compliance with data subject's rights in the report on the situation of human rights and freedoms in Mongolia.

24.2. One member of the National Human Rights Commission shall be specifically responsible for the functions specified in Paragraph 24.1 of this Law.

Article 25. Full Power of the State Central Administrative Body in charge of Digital Development and Communication Regarding Data Protection in the Digital Environment

25.1. The state central administrative body in charge of digital development and communication shall exercise the following full powers for the data protection in the digital environment:

25.1.1. Ensure the implementation of the laws on personal data protection, raise public awareness, and organize advocacy activities, cooperate with relevant organizations, and provide professional and methodological assistance.

25.1.2. Approve technological security requirements and procedures for processing sensitive personal data, genetic and biometric data.

25.1.3. Receive and register the data subject's report of security failures of information system intended for data collection, processing and use, occurrence of cyber-attacks, and immediately take necessary measures.

Article 26. Full Power of Other State Authorities for Information Protection

26.1. The state authority shall monitor the data collection, processing and use by the data controller within the scope of its functions specified in the applicable laws.

Chapter seven

audio, video and audio Video recording system

Article 27. Audio, Video and Audio-Video Recording System

27.1. Audio, video, and audio-video recording equipment consists of fixed and mobile technical instrument that can collect, transmit, and store audio, video, and audio-video data with technological assistance.

27.2. Audio, video, and audio-video recording system shall consist of equipment, data transmission network, storage device and software specified in Paragraph 27.1 of this Law.

27.3. Unless otherwise provided by Law, video recording devices may be installed for following purposes:

27.3.1. Protect the safety of residents at the entrances and exits of public housing and common areas and ensure the safety of shared properties.

27.3.2. Protect people and ensure information security in the workplace and ensure the safety of the properties of organizations.

27.3.3. Collect, process, use and analyze traffic information.

27.4. Unless otherwise provided by law, the following activities shall be prohibited for the installation of video recording equipment and use of video recordings under Paragraph 27.3 of this Law, including:

27.4.1. Install video recording equipment in locations where the right to personal liberty and immunity will be clearly violated such as toilets, dressing rooms, special purpose service rooms of commercial areas, karaoke rooms, hotel rooms, and inpatient rooms for the provision of healthcare services.

27.4.2. Install video recording equipment covering the entrances and exits of households residing in public apartments.

27.4.3. Distribute video recordings of public entrances and exits of public housing and common areas to the mass media.

27.4.4. Show and copy the video recordings, if the video recording contains information of a person other than the data subject.

27.5. Installation of audio and audio-video recording devices is prohibited in the places specified in Sub-paragraphs 27.3.1, 27.4.1 and 27.4.2 of this Law.

27.6. The warnings of audio, video and audio-video recording devices shall be placed in visible areas for the citizens.

27.7. The state central administrative body in charge of digital development and communication shall determine the information which will be specified in the requirements and warnings for the installation of audio, video and audio-video recording devices based on the proposal of the National Human Rights Commission.

27.8. The National Human Rights Commission may conduct inspections in cooperation with law enforcement agencies in order to monitor the activities specified in Paragraphs 27.3 and 27.4 of this Law and the lawful use of audio, video, and audio-visual recording systems under other laws.

27.9. Under the procedures set forth in the law, the data controller may review, show, and listen to the data contained in the audio, video, and audio-video recording system, and copy the stored recordings for the authorized organization or official.

27.10. The audio, video and audio-video recording system shall have technical and operational conditions in place to prevent authorized access to data.

CHAPTER EIGHT MISCELLANEOUS

Article 28. Resolving Complaints of Data Subjects

28.1. The data subject shall file a complaint related to the data collection, processing and use by the state organization for resolution under the General Administrative Law and other applicable laws.

28.2. Except the complaint specified in Paragraph 28.1 of this Law, the complaints related to the data controller's data collection, processing and use shall be submitted to and resolved by the competent authority or the National Human Rights Commission.

28.3. The data subject who is disagreement with the decision specified in Paragraphs 28.1 and 28.2 of this Law may appeal to the court.

Article 29. Prohibitions

29.1. It is prohibited to collect, process, or use data from the data subject for purposes other than those specified in the Law or for purposes different from the initial purpose.

29.2. It is prohibited to violate the rights and freedoms of the data subject during the electronic data processing without any human intervention.

29.3. It shall be prohibited for a person who acquired the data under this law to disclose the data to others.

Article 30. Liability for the Violation of the Law

30.1. The official in violation of this Law whose actions are not of a criminal nature shall be subject to liability as specified in the Law on Civil Service or the Labor Code.

30.2. A person or legal entity that violates this Law shall be subject to liability specified in the Criminal Code or the Law on Violations.

Article 31. Transfer Arrangements

31.1. Prior to the entry into force of this law, non-overlapping physiological data (fingerprints) collected by the data controller, other than those permitted by law, shall be erased.

31.2. A working group shall be established by the decision of the Government for the organization and monitoring of the activities specified in Paragraph 31.1 of this Law.

Article 32. Entry into Force

32.1. The law shall come into force on May 1, 2022.

THE CHAIRMAN OF THE STATE GREAT KHURAL OF MONGOLIA ZANDANSHATAR.G