AN ACT relating to insurance data security.

Be it enacted by the General Assembly of the Commonwealth of Kentucky:

➔SECTION 1. A NEW SECTION OF SUBTITLE 3 OF KRS CHAPTER 304 IS CREATED TO READ AS FOLLOWS:

As used in Sections 1 to 10 of this Act:

(1) "Consumer" means an individual, including but not limited to an applicant, policyholder, insured, beneficiary, claimant, and certificate holder:

(a) Who is a resident of this Commonwealth; and

(b) Whose nonpublic information is in a licensee's possession, custody, or control;

(2) "Cybersecurity event":

(a) Means an event resulting in unauthorized access to, disruption of, or misuse of an information system or nonpublic information stored on an information system; and

(b) Shall not include:

1. Unauthorized acquisition of encrypted nonpublic information if the encryption, process, or key is not also acquired, released, or used without authorization; or

2. An event with regard to which the licensee has determined that the nonpublic information accessed by an unauthorized person:

a. Has not been used or released; and

b. Has been returned or destroyed;

(3) "Encrypted" means the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key;

(4) "Information security program" means the administrative, technical, and physical safeguards that a licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle nonpublic

information;

(5) "Information system":

(a) Means a discrete set of electronic nonpublic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of electronic information; and

(b) Shall include any specialized system such as industrial or process controls systems, telephone switching and private branch exchange systems, and environmental control systems;

(6) "Licensee":

(a) Means any person who is, or is required to be, licensed, authorized to operate, or registered pursuant to the insurance laws of this state; and

(b) Shall not include:

1. A purchasing group or a risk retention group chartered and licensed in a state other than this state; or

2. A licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction;

(7) "Nonpublic information":

(a) Means electronic information that is not publicly available information; and

(b) Shall include:

1. Business-related information of a licensee that if tampered with, or disclosed, accessed, or used without authorization, would cause a material adverse impact to the business, operations, or security of the licensee;

2. Any confidential personal identifying information of a consumer, including:

a. Social Security number;

b. Operator's license number or personal identification card number;

c. Financial account number;

d. Credit or debit card number;

e. Any security code, access code, or password that would permit access to a consumer's financial account; or

f. Biometric records; and

3. Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or a consumer that relates to:

a. The past, present, or future physical, mental, or behavioral health or condition of any consumer or member of the consumer's family;

b. The provision of health care to any consumer; or

c. Payment for the provision of health care to any consumer;

(8) "Person" means any individual or nongovernmental entity, including but not limited to any nongovernmental partnership, corporation, branch, agency, or association;

(9) (a) "Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from:

1. Federal, state, or local government records;

2. Widely distributed media; or

3. Disclosures to the general public that are required to be made by federal, state, or local law.

(b) For purposes of this definition, a licensee has a reasonable basis to believe that information is lawfully made available to the general public if the

licensee has taken steps to determine:

1. That the information is of the type that is available to the general public; and

2. Whether the consumer can direct that information not be made available to the general public, and if so, that the consumer has not done so; and

(10) "Third-party service provider" means a person, other than a licensee, that:

(a) Contracts with a licensee to maintain, process, or store nonpublic information; or

(b) Is otherwise permitted access to nonpublic information through its provision of services to a licensee.

➔SECTION 2. A NEW SECTION OF SUBTITLE 3 OF KRS CHAPTER 304 IS CREATED TO READ AS FOLLOWS:

A licensee with fewer than fifty (50) employees, including independent contractors, shall be exempt from the requirements of Sections 1 to 10 of this Act.

➔SECTION 3. A NEW SECTION OF SUBTITLE 3 OF KRS CHAPTER 304 IS CREATED TO READ AS FOLLOWS:

Notwithstanding any other law, Sections 1 to 10 of this Act establish the exclusive requirements applicable to licensees, except licensees exempt under Section 2 of this Act, under the laws of the Commonwealth of Kentucky for:

(1) Data security;

(2) The investigation of a cybersecurity event; and

(3) Notification to the commissioner regarding the occurrence of a cybersecurity event.

➔SECTION 4. A NEW SECTION OF SUBTITLE 3 OF KRS CHAPTER 304 IS CREATED TO READ AS FOLLOWS:

(1) As used in this section:

(a) "Authorized individual" means an individual:

1. Known to, and screened by, the licensee; and

2. Determined to be necessary and appropriate to have access to the nonpublic information held by the licensee and its information systems;

(b) "Multi-factor authentication" means authentication through verification of at least two (2) of the following methods of authentication factors:

1. Knowledge factors, such as a password;

2. Possession factors, such as a token or text message on a mobile phone; or

3. Inherence factors, such as a biometric characteristic; and

(c) "Risk assessment" means the risk assessment that each licensee is required to conduct under subsection (3) of this section.

(2) (a) Each licensee shall develop, implement, and maintain a comprehensive written information security program based on the licensee's risk assessment that contains administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system.

(b) The information security program required under this subsection shall be:

1. Commensurate with the:

a. Size and complexity of the licensee;

b. Nature and scope of the licensee's activities, including its use of third-party service providers; and

c. Sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control; and

2. Designed to:

a. Protect the security and confidentiality of nonpublic information

and the security of the information system;

b. Protect against any threats or hazards to the security or integrity of nonpublic information and the information system;

c. Protect against unauthorized access to or use of nonpublic information and minimize the likelihood of harm to any consumer; and

d. Define, and periodically reevaluate:

i. A schedule for retention of nonpublic information; and

ii. A mechanism for the destruction of nonpublic information when no longer needed, which shall comply with KRS 365.725.

(3) Each licensee shall:

(a) Designate one (1) or more employees, an affiliate, or an outside vendor designated to act on behalf of the licensee who is responsible for the information security program;

(b) Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration, or destruction of nonpublic information, including the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers;

(c) Assess the likelihood and potential damage of the threats identified under paragraph (b) of this subsection, taking into consideration the sensitivity of the nonpublic information;

(d) Assess the sufficiency of policies, procedures, information systems, and other safeguards in place to manage the threats identified under paragraph (b) of this subsection, including consideration of threats in each relevant area of the licensee's operations, including:

1. Employee training and management;

2. Information systems, including network and software design, information classification, governance, processing, storage, transmission, and disposal; and

3. Detection, prevention, and response to attacks, intrusions, or other system failures;

(e) Implement information safeguards to manage the threats identified in the licensee's ongoing assessment; and

(f) No less than annually, assess the effectiveness of the key controls, systems, and procedures of the safeguards implemented under paragraph (e) of this subsection.

(4) Based on its risk assessment, each licensee shall:

(a) Design its information security program to mitigate the identified risks commensurate with the:

1. Size and complexity of the licensee; and

2. Nature and scope of the licensee's activities, including its use of third-party service providers;

(b) Implement the following security measures, as appropriate:

1. Place access controls on information systems, including controls to authenticate and permit access only to authorized individuals to protect against the unauthorized acquisition of nonpublic information;

2. Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy;

3. Restrict physical access to nonpublic information to authorized

individuals only;

4. Protect, by encryption or other appropriate means, all nonpublic information:

a. While being transmitted over an external network; and

b. Stored on a laptop computer or other portable computing or storage device or media;

5. Adopt:

a. Secure development practices for in-house developed applications utilized by the licensee; and

b. Procedures for evaluating, assessing, or testing the security of externally developed applications utilized by the licensee;

6. Modify the information system in accordance with the licensee's information security program;

7. Utilize effective controls, which may include multi-factor authentication procedures for any individual accessing nonpublic information;

8. Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;

9. Include audit trails within the information security program designed to:

a. Detect and respond to cybersecurity events; and

b. Reconstruct material financial transactions sufficient to support normal operations and obligations of the licensee;

10. Implement measures to protect against destruction, loss, or damage of nonpublic information due to environmental hazards, such as fire and water damage, or other catastrophes or technological failures; and

11. Develop, implement, and maintain procedures for the secure disposal

of nonpublic information in any format;

(c) Include cybersecurity risks in the licensee's enterprise risk management process;

(d) Stay informed regarding emerging threats or vulnerabilities;

(e) Utilize reasonable security measures when sharing information commensurate with the character of the sharing and the type of information shared; and

(f) Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the licensee in its risk assessment.

(5) (a) A licensee's executive management or its delegates shall, at a minimum:

1. Develop, implement, and maintain the licensee's information security program; and

2. If the licensee has a board of directors or other appropriate committee, report at least annually, in writing, to the board or committee the following information:

a. The overall status of the information security program and the licensee's compliance with Sections 1 to 10 of this Act; and

b. Material matters related to the information security program, addressing issues including risk assessment, risk management and control decisions, third-party service provider arrangements, results of testing, cybersecurity events or violations and management's response to the events or violations, and recommendations for changes in the information security program.

(b) If a licensee's executive management delegates any of its responsibilities under this subsection, executive management shall:

1. Oversee the development, implementation, and maintenance of the

licensee's information security program prepared by the delegate or delegates; and

2. Receive a report from the delegate or delegates that complies with the requirements of paragraph (a)2. of this subsection.

(6) Each licensee that uses a third-party service provider shall:

(a) Exercise due diligence in selecting the third-party service provider; and

(b) Require the third-party service provider to implement appropriate administrative, technical, and physical measures to protect and secure the information systems and nonpublic information that are accessible to, or held by, the third-party service provider.

(7) Each licensee shall monitor, evaluate, and adjust, as appropriate, the information security program consistent with:

(a) Any relevant changes in technology;

(b) The sensitivity of its nonpublic information;

(c) Internal or external threats to information; and

(d) The licensee's own changing business arrangements, including mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

(8) (a) As part of its information security program, each licensee shall establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event that compromises:

1. The confidentiality, integrity, or availability of nonpublic information in its possession;

2. The licensee's information systems; or

3. The continuing functionality of any aspect of the licensee's business or operations.

(b) The incident response plan established under this subsection shall address

the following:

1. The internal process for responding to a cybersecurity event;

2. The goals of the incident response plan;

3. The definition of clear roles, responsibilities, and levels of decision-making authority;

4. External and internal communications and information sharing;

5. Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

6. Documentation and reporting regarding cybersecurity events and related incident response activities; and

7. The evaluation and revision, as necessary, of the incident response plan following a cybersecurity event.

(9) (a) Each insurer domiciled in this state shall:

1. By February 15 of each year, submit to the commissioner a written statement certifying that the insurer is in compliance with this section; and

2. Maintain, for examination by the department, all records, schedules, and data supporting the certification submitted under subparagraph 1. of this paragraph for a period of five (5) years.

(b) 1. To the extent an insurer has identified areas, systems, or processes that require material improvement, updating, or redesign, the insurer shall document the identification and remedial efforts planned and underway to address the areas, systems, or processes identified.

2. The documentation required under this paragraph shall be available for inspection by the commissioner for a period of five (5) years.

(10) (a) An employee, agent, representative, or designee of a licensee, who is also a licensee, shall be exempt from the requirements of this section and shall not

be required to develop its own information security program to the extent that the employee, agent, representative, or designee is covered by the information security program of the other licensee.

(b) In the event that a licensee ceases to qualify for an exception under paragraph (a) of this subsection, the licensee shall have one hundred eighty (180) days to comply with this section.

➔SECTION 5. A NEW SECTION OF SUBTITLE 3 OF KRS CHAPTER 304 IS CREATED TO READ AS FOLLOWS:

(1) (a) If a licensee learns that a cybersecurity event has or may have occurred, the licensee, or an outside vendor or service provider designated to act on behalf of the licensee, shall conduct a prompt investigation.

(b) During an investigation required under this subsection, the licensee, or outside vendor or service provider designated to act on behalf of the licensee, shall, at a minimum:

1. Determine whether a cybersecurity event has occurred;

2. Assess the nature and scope of the cybersecurity event;

3. Identify any nonpublic information that may have been involved in the cybersecurity event; and

4. Perform or oversee reasonable measures to restore the security of the information systems compromised in the cybersecurity event in order to prevent further unauthorized acquisition, release, or use of nonpublic information in the licensee's possession, custody, or control.

(2) If a licensee learns that a cybersecurity event has or may have occurred in a system maintained by a third-party service provider, the licensee shall complete, or confirm and document that the third-party service provider has completed, the steps listed in subsection (1)(b) of this section.

(3) Each licensee shall maintain, and produce upon demand of the commissioner, records concerning all cybersecurity events for a period of at least five (5) years from the date of the cybersecurity event.

➔SECTION 6. A NEW SECTION OF SUBTITLE 3 OF KRS CHAPTER 304 IS CREATED TO READ AS FOLLOWS:

(1) Each licensee shall notify the commissioner of a cybersecurity event involving nonpublic information that is in the possession of the licensee as promptly as possible, but in no event later than three (3) business days from a determination that a cybersecurity event has occurred, if:

(a) In the case of an insurer, this state is the licensee's state of domicile and the cybersecurity event has a reasonable likelihood of harming any material part of normal operations of the licensee;

(b) In the case of an insurance producer, this state is the licensee's home state, as those terms are defined in KRS 304.9-020; or

(c) The licensee reasonably believes that:

1. The nonpublic information involved in the cybersecurity event is related to two hundred fifty (250) or more consumers residing in this state; and

2. The cybersecurity event is either of the following:

a. A cybersecurity event requiring the licensee to provide notice to any governmental body, self-regulatory agency, or any other supervisory body pursuant to any state or federal law; or

b. A cybersecurity event that has a reasonable likelihood of materially harming any:

i. Consumer residing in this state; or

ii. Material part of the normal operations of the licensee.

(2) (a) In its notification to the commissioner under subsection (1) of this section,

the licensee shall provide, in an electronic form prescribed by the commissioner, the following information:

1. The date of the cybersecurity event;

2. A description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers, if any;

3. How the cybersecurity event was discovered;

4. Whether any lost, stolen, or breached information has been recovered, and if so, how the information was recovered;

5. The identity of the source of the cybersecurity event;

6. Whether the licensee has filed a police report or has notified any regulatory, government, or law enforcement agencies, and if so, when the notification was provided;

7. A description of the specific types of information acquired without authorization, including but not limited to types of medical information, financial information, or information allowing identification of the consumer;

8. The period during which the information system was compromised by the cybersecurity event;

9. The licensee's best estimate of the number of total consumers in this state affected by the cybersecurity event, which shall be updated with each subsequent report to the commissioner pursuant to this section;

10. The results of any internal review:

a. Identifying a lapse in automated controls or internal procedures; or

b. Confirming that all automated controls or internal procedures were followed;

11. A description of the efforts being undertaken to remediate the situation that permitted the cybersecurity event to occur;

12. A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the cybersecurity event;

13. A copy of the notice sent to consumers under KRS 365.732, if applicable; and

14. The name of a contact person who is familiar with the cybersecurity event and authorized to act for the licensee.

(b) The licensee shall have a continuing obligation under subsection (1) of this section to update and supplement initial and subsequent notifications to the commissioner concerning the cybersecurity event.

(3) Each licensee shall comply with KRS 365.732, as applicable.

(4) In the case of a cybersecurity event in a system maintained by a third-party service provider of which the licensee has become aware:

(a) Except as provided under subsection (5) of this section, the licensee shall treat the cybersecurity event as it would under subsection (1) of this section; and

(b) The computation of the licensee's deadlines under this subsection shall begin on the earlier of the day after:

1. The third-party service provider notifies the licensee of the cybersecurity event; or

2. The licensee otherwise has actual knowledge of the cybersecurity event.

(5) Nothing in Sections 1 to 10 of this Act shall prevent or abrogate an agreement between a licensee and another licensee, a third-party service provider, or any other party to fulfill the obligations of or obligations similar to:

(a) Investigation requirements under Section 5 of this Act; or

(b) Notice requirements under this section.

(6) (a) In the case of a cybersecurity event involving nonpublic information that is used by a licensee acting as an assuming insurer, or that is in the possession, custody, or control of a licensee that is acting as an assuming insurer, and the assuming insurer does not have a direct contractual relationship with the affected consumers, the assuming insurer shall notify its affected ceding insurers and the commissioner of its state of domicile within three (3) business days of making the determination that a cybersecurity event has occurred.

(b) In the case of a cybersecurity event involving nonpublic information that is in the possession, custody, or control of a third-party service provider of a licensee that is an assuming insurer, the assuming insurer shall notify its affected ceding insurers and the commissioner of its state of domicile within three (3) business days of receiving notice from its third-party service provider that a cybersecurity event has occurred.

(c) A ceding insurer under paragraphs (a) or (b) of this subsection that has a direct contractual relationship with affected consumers shall fulfill:

1. The consumer notification requirements imposed under KRS 365.732; and

2. Any other notification requirements relating to a cybersecurity event under this section.

(d) Except as provided in paragraphs (a) or (b) of this subsection, a licensee acting as an assuming insurer shall not be subject to any notice obligations relating to a cybersecurity event or other data breach under this section.

(7) (a) Except as provided in paragraph (b) of this subsection, in the case of a cybersecurity event involving nonpublic information that is in the

possession, custody, or control of a licensee that is an insurer, or its third-party service provider, and for which a consumer accessed the insurer's services through an independent insurance producer, the insurer shall notify the producers of record at the same time as all affected consumers when a licensee is required to notify consumers under KRS 365.732.

(b) An insurer shall not be required to comply with paragraph (a) of this subsection when the insurer does not have the current producer of record information for any individual consumer.

➔SECTION 7. A NEW SECTION OF SUBTITLE 3 OF KRS CHAPTER 304 IS CREATED TO READ AS FOLLOWS:

(1) (a) The commissioner shall have the power to examine and investigate the affairs of any licensee to determine whether the licensee has been or is engaged in any conduct in violation of Section 4, 5, or 6 of this Act.

(b) The power granted to the commissioner under this subsection shall be in addition to the powers of the commissioner under KRS 304.2-100.

(c) Any investigation or examination conducted under this subsection shall be conducted pursuant to KRS 304.2-210.

(2) If the commissioner has reason to believe that a licensee has been or is engaged in conduct in this state that violates Section 4, 5, or 6 of this Act, the commissioner may take action that is necessary or appropriate to enforce the relevant provisions.

➔SECTION 8. A NEW SECTION OF SUBTITLE 3 OF KRS CHAPTER 304 IS CREATED TO READ AS FOLLOWS:

(1) (a) Subject to paragraph (b) of this subsection and subsections (3) and (6) of this section, any documents, materials, or other information in the control or possession of the department that are furnished by a licensee, or an employee or agent acting on behalf of a licensee, under Section 4, 5, or 6 of

this Act or that are obtained by the commissioner in an investigation or examination under Section 7 of this Act shall:

1. Be confidential by law and privileged;

2. Not be subject to KRS 61.870 to 61.884;

3. Not be subject to subpoena; and

4. Not be subject to discovery or admissible in evidence in any private civil action.

(b) The commissioner may use documents, materials, or other information referenced under paragraph (a) of this subsection in furtherance of any regulatory or legal action brought as part of the commissioner's duties, and shall not otherwise make the documents, materials, or other information public without the written consent of the licensee.

(2) The commissioner, and any person who received documents, materials, or other information while acting under the authority of the commissioner, shall not be permitted, or required, to testify in any private civil action concerning any confidential documents, materials, or other information subject to subsection (1)(a) of this section.

(3) In order to assist in the performance of the commissioner's duties under Sections 1 to 10 of this Act, the commissioner:

(a) May share documents, materials, and other information, including confidential and privileged documents, materials, or other information subject to subsection (1) of this section, with the following if the recipient agrees, in writing, to maintain the confidentiality and privileged status of the documents, materials, or other information:

1. State, federal, and international regulatory agencies;

2. The National Association of Insurance Commissioners, its affiliates, or subsidiaries; and

3. State, federal, and international law enforcement authorities;

(b) May receive documents, materials, and other information, including confidential and privileged documents, materials, or information, from:

1. The National Association of Insurance Commissioners, its affiliates, or subsidiaries; and

2. Regulatory and law enforcement officials of other foreign and domestic jurisdictions;

(c) Shall maintain as confidential and privileged any document, material, or information received with notice or understanding that it is confidential and privileged under the laws of the jurisdiction that is the source of the documents, materials, or other information;

(d) May share documents, materials, and other information subject to subsection (1) this section with a third-party consultant or vendor, if the consultant or vendor agrees, in writing, to maintain the confidentiality and privileged status of the documents, materials, or other information; and

(e) May enter into agreements governing the sharing and use of information consistent with this section.

(4) No waiver of any applicable privilege or claim of confidentiality shall occur as a result of:

(a) A disclosure to the commissioner of documents, materials, or other information under this section; or

(b) The sharing of the documents, materials, or other information as authorized under subsection (3) of this section.

(5) Documents, materials, and other information in the possession or control of the National Association of Insurance Commissioners or a third-party consultant or vendor pursuant to Sections 1 to 10 of this Act shall:

(a) Be confidential by law and privileged;

(b) Not be subject to KRS 61.870 to 61.884;

(c) Not be subject to subpoena; and

(d) Not be subject to discovery or admissible in evidence in any private civil action.

(6) Nothing in Sections 1 to 10 of this Act shall prohibit the commissioner from releasing final, adjudicated actions that are open to public inspection under KRS 304.2-150 to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates, or subsidiaries.

➔SECTION 9. A NEW SECTION OF SUBTITLE 3 OF KRS CHAPTER 304 IS CREATED TO READ AS FOLLOWS:

(1) A licensee shall be deemed in compliance with Sections 1 to 10 of this Act if the licensee:

(a) 1. Is subject to, governed by, and compliant with the privacy, security, and breach notifications rules issued by the United States Department of Health and Human Services, 45 C.F.R. Parts 160 and 164, as amended, established pursuant to the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, as amended, and the Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, as amended;

2. Maintains nonpublic information in the same manner as protected health information; and

3. Submits to the commissioner:

a. An annual written statement certifying its compliance with the applicable provisions referenced under subparagraph 1. of this paragraph; and

b. A copy of any individual breach notification required under 45 C.F.R. sec. 164.404, as amended, at the same time as all affected

individuals; or

(b) 1. Is a financial institution, as defined in KRS 304.9-135, that is subject to, governed by, and compliant with the privacy, security, and breach notification standards issued under Section 501 of the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. sec. 6801, as amended; and

2. Submits to the commissioner:

a. An annual written statement certifying its compliance with the applicable provisions referenced under subparagraph 1. of this paragraph; and

b. A copy of any breach notification at the same time and in the same manner as notifications provided to the financial institution's federal regulatory authorities.

(2) Nothing in subsection (1)(a) of this section shall be construed to restrict the commissioner's authority to examine and investigate the affairs of any licensee under Section 7 of this Act to verify the licensee's annual certification under this section.

➔SECTION 10. A NEW SECTION OF SUBTITLE 3 OF KRS CHAPTER 304 IS CREATED TO READ AS FOLLOWS:

Penalties for violations of Sections 1 to 10 of this Act shall be in accordance with KRS 304.99-020.

➔Section 11. Pursuant to KRS 304.2-110, the commissioner may promulgate administrative regulations necessary for or as an aid to the effectuation of this Act.

➔Section 12. If any provision of this Act or application thereof to any person or circumstance is for any reason held to be invalid, the invalidity shall not affect the remainder of the Act or the application of the provision to other persons or circumstances, and to this end the provisions of this Act are severable.

➔Section 13. (a) Licensees shall have one year from the effective date of this

Act to implement subsections (1) to (3) and subsections (5) to (7) of Section 4 of this Act.

(b) Licensees shall have two years from the effective date of this Act to implement subsection (4) of Section 4 of this Act.

➔Section 14. This Act takes effect January 1, 2023.