Code of Ala. § 27-62-5

Current through the end of the 2023 First Special, Regular, and Second Special Sessions, but not including corrections and changes made to the 2023 session laws by the Code Commissioner.

Michie's™ Alabama Code > TITLE 27 Insurance (Chs. 1 — 64) > CHAPTER 62 Insurance Data Security Law (§§ 27-62-1 — 27-62-11)

§ 27-62-5. Investigation of a cybersecurity event.

(a) If the 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 the investigation, the licensee, or an outside vendor or service provider designated to act on behalf of the licensee, at a minimum, shall determine as much of the following information as possible:

(1) If a cybersecurity event has occurred.

(2) The nature and scope of the cybersecurity event.

(3) Any nonpublic information that may have been involved in the cybersecurity event.

(c) The licensee shall 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 possession, custody, or control of the licensee.

(d) If the 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 the steps listed in subsection (b) or confirm and document that the third-party service provider has completed those steps.

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

History

Acts 2019, No. 19-98, § 5, effective May 1, 2019.

End of Document

Code of Ala. § 27-62-6

Current through the end of the 2023 First Special, Regular, and Second Special Sessions, but not including corrections and changes made to the 2023 session laws by the Code Commissioner.

§ 27-62-6. Notification of a cybersecurity event.

(a) Each licensee shall notify the commissioner as promptly as possible, but in no event later than three business days from a determination that a cybersecurity event involving nonpublic information that is in the possession of a licensee has occurred when either of the following criteria has been met:

(1) This state is the state of domicile of the licensee, in the case of an insurer, or this state is the home state of the licensee, in the case of a producer, as those terms are defined in Section 27-7-1, and the cybersecurity event has a reasonable likelihood of materially harming a consumer residing in this state or reasonable likelihood of materially harming any material part of the normal operation of the licensee.

(2) The licensee reasonably believes that the nonpublic information involves 250 or more consumers residing in this state and the cybersecurity event is either of the following:

a. A cybersecurity event impacting the licensee that the licensee is required to notify any government body, self-regulatory agency, or any other supervisory body about pursuant to any state or federal law.

b. A cybersecurity event that has a reasonable likelihood of materially harming either of the following:

1. Any consumer residing in this state.

2. Any material part of the normal operation of the licensee.

(b) The licensee shall provide as much of the following information as possible in electronic form as directed by the commissioner:

(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 any third-party service providers.

(3) How the cybersecurity event was discovered.

(4) Whether any lost, stolen, or breached information has been recovered and if so, how this was done.

(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. Specific types of information means particular data elements including, for example, types of medical information, types of financial information, or types of information allowing identification of the consumer.

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

(9) The number of total consumers in this state affected by the cybersecurity event. The licensee shall provide the best estimate in the initial report to the commissioner and update this estimate with each subsequent report to the commissioner pursuant to this section.

(10) The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed.

(11) A description of efforts being undertaken to remediate the situation which permitted the cybersecurity event to occur.

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

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

(c) The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications regarding material changes to previously provided information relating to the cybersecurity event.

(d) The licensee shall comply with the Alabama Data Breach Notification Act of 2018, Chapter 38 of Title 8, as applicable and provide a copy of the notice sent to consumers under the law to the commissioner.

(e)

(1) If the licensee becomes aware of a cybersecurity event in a system maintained by a third-party service provider, the licensee shall treat the event in the same manner as provided under subsection (a) unless the third-party service provider provides the notice required under subsection (a) to the commissioner.

(2) The computation of deadlines of a licensee shall begin on the day after the third-party service provider notifies the licensee of the cybersecurity event or the licensee otherwise has actual knowledge of the cybersecurity event, whichever is sooner.

(3) Nothing in this chapter shall prevent or abrogate an agreement between a licensee and another licensee, a third-party service provider, or any other party to fulfill any of the investigation requirements of Section 27-62-5 or the notice requirements of this section.

(f)

(1)

a. In the case of a cybersecurity event involving nonpublic information that is used by the licensee that is acting as an assuming insurer or in the possession, custody, or control of a licensee that is acting as an assuming insurer and that 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 business days of making the determination that a cybersecurity event has occurred.

b. The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements under the Alabama Data Breach Notification Act of 2018, Chapter 38 of Title 8, and any other notification requirements relating to a cybersecurity event under this section.

(2)

a. 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 business days of receiving notice from its third-party service provider that a cybersecurity event has occurred.

b. The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements under the Alabama Data Breach Notification Act of 2018, Chapter 38 of Title 8, and any other notification requirements relating to a cybersecurity event under this section.

(3) Any licensee acting as assuming insurer shall have no other notice obligations relating to a cybersecurity event or other data breach under this section or any other law of this state.

(g)

(1) 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 for which a consumer accessed the services of the insurer through an independent insurance producer, and for which consumer notice is required by the Alabama Data Breach Notification Act of 2018, Chapter 38 of Title 8, the insurer shall notify the producers of record of all affected consumers of the cybersecurity event no later than the time at which notice is provided to the affected consumers.

(2) The insurer is excused from this obligation for any producers who are not authorized by law or contract to sell, solicit, or negotiate on behalf of the insurer, and in those instances in which the insurer does not have the current producer of record information for an individual consumer.

History

Acts 2019, No. 19-98, § 6, effective May 1, 2019.

Code of Ala. § 27-62-4

Current through the end of the 2023 First Special, Regular, and Second Special Sessions, but not including corrections and changes made to the 2023 session laws by the Code Commissioner.

Michie's™ Alabama Code > TITLE 27 Insurance (Chs. 1 — 64) > CHAPTER 62 Insurance Data Security Law (§§ 27-62-1 — 27-62-11)

§ 27-62-4. Information security program.

(a) Commensurate with the size and complexity of the licensee, the nature and scope of the activities of the licensee, including its use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the possession, custody, or control of the licensee, each licensee shall develop, implement, and maintain a comprehensive written information security program based on the risk assessment of the licensee that contains administrative, technical, and physical safeguards for the protection of nonpublic information and the information system of the licensee.

(b) The information security program of a licensee shall be designed to do all of the following:

(1) Protect the security and confidentiality of nonpublic information and the security of the information system.

(2) Protect against any threats or hazards to the security or integrity of nonpublic information and the information system.

(3) Protect against unauthorized access to or use of nonpublic information and minimize the likelihood of harm to any consumer.

(4) Define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for its destruction when no longer needed.

(c) The licensee shall do all of the following:

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

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

(3) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the nonpublic information.

(4) Assess the sufficiency of policies, procedures, information systems, and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the operations of the licensee, including all of the following:

a. Employee training and management.

b. Information systems, including network and software design, as well as information classification, governance, processing, storage, transmission, and disposal.

c. Detecting, preventing, and responding to attacks, intrusions, or other systems failures.

(5) Implement information safeguards to manage the threats identified in its ongoing assessment, and no less than annually, assess the effectiveness of the key controls, systems, and procedures of the safeguards.

(d) Based on its risk assessment, the licensee shall do all of the following:

(1) Design its information security program to mitigate the identified risks commensurate with the size and complexity of the licensee, the nature and scope of the activities of the licensee, including the use by the licensee of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the possession, custody, or control of the licensee.

(2) Determine which security measures listed below are appropriate and, if appropriate, do the following to implement the security measures:

a. 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.

b. 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 risk strategy of the licensee.

c. Restrict physical access to nonpublic information to authorized individuals only.

d. Protect by encryption or other appropriate means, all nonpublic information while being transmitted over an external network and all nonpublic information stored on any laptop computer or other portable computing or storage device or media.

e. Adopt secure development practices for in-house developed applications utilized by the licensee.

f. Modify the information system in accordance with the information security program of the licensee.

g. Utilize effective controls, which may include multi-factor authentication procedures for employees accessing nonpublic information.

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

i. Include audit trails within the information security program designed to detect and respond to cybersecurity events and designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the licensee.

j. 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.

k. Develop, implement, and maintain procedures for the secure disposal of nonpublic information in any format.

(3) Include cybersecurity risks in the enterprise risk management process of the licensee.

(4) Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared.

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

(e) If the licensee has a board of directors, the board or an appropriate committee of the board, at a minimum, shall do all of the following:

(1) Require the executive management of the licensee or its delegates to develop, implement, and maintain the information security program of the licensee.

(2) Require the executive management of the licensee or its delegates to report in writing at least annually, all of the following:

a. The overall status of the information security program of the licensee and the compliance of the licensee with this chapter.

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

(3) If executive management delegates any of its responsibilities under this section, it shall oversee the development, implementation, and maintenance of the information security program of the licensee prepared by the delegate and shall receive a report from the delegate complying with the requirements of the report to the board of directors.

(f)

(1) A licensee shall exercise due diligence in selecting a third-party service provider.

(2) A licensee shall require a 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.

(g) The licensee shall monitor, evaluate, and adjust, as appropriate, the information security program consistent with any relevant changes in technology, the sensitivity of its nonpublic information, internal or external threats to information, and the changing business arrangements of the licensee, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.

(h)

(1) 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 the confidentiality, integrity, or availability of nonpublic information in its possession, the information systems of the licensee, or the continuing functionality of any aspect of the business or operations of the licensee.

(2) The incident response plan shall address all of the following areas:

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

b. The goals of the incident response plan.

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

d. External and internal communications and information sharing.

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

f. Documentation and reporting regarding cybersecurity events and related incident response activities.

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

(i) Each insurer domiciled in this state, annually on or before February 15, shall submit to the commissioner a written statement certifying that the insurer is in compliance with the requirements set forth in this chapter. Each insurer shall maintain for examination by the department all records, schedules, and data supporting this certificate for a period of five years. 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 the remedial efforts planned and underway to address the areas, systems, or processes. The documentation shall be available for inspection by the commissioner.

(j) Licensees shall have until May 1, 2021, to implement subsection (f) and until May 1, 2020, to implement the remainder of this section.

History

Acts 2019, No. 19-98, §§ 4, 14, effective May 1, 2019.

Code of Ala. § 27-62-3

Current through the end of the 2023 First Special, Regular, and Second Special Sessions, but not including corrections and changes made to the 2023 session laws by the Code Commissioner.

Michie's™ Alabama Code > TITLE 27 Insurance (Chs. 1 — 64) > CHAPTER 62 Insurance Data Security Law (§§ 27-62-1 — 27-62-11)

§ 27-62-3. Definitions.

For purposes of this chapter, the following words have the following meanings:

(1) Authorized individual. An individual known to and screened by the licensee and determined to be necessary and appropriate to have access to the nonpublic information held by the licensee and its information systems.

(2) Commissioner. The Commissioner of Insurance.

(3) Consumer. An individual, including, but not limited to, an applicant, policyholder, insured, beneficiary, claimant, or certificate holder, who is a resident of this state and whose nonpublic information is in the possession, custody, or control of a licensee.

(4)

a. Cybersecurity event. An event resulting in unauthorized access to, disruption, or misuse of an information system or nonpublic information stored on an information system.

b. The term cybersecurity event does not include the unauthorized acquisition of encrypted nonpublic information if the encryption, process, or key is not also acquired, released, or used without authorization.

c. Cybersecurity event does not include an event with regard to which the licensee has determined that the nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed.

(5) Department. The Department of Insurance.

(6) Encrypted. The transformation of data into a form which results in a low probability of assigning meaning without the use of a protective process or key.

(7) Information security program. 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.

(8) Information system. A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of electronic nonpublic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

(9) Licensee. Any person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this state but shall not include a purchasing group or a risk retention group chartered and licensed in a state other than this state or a licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction.

(10) Multi-factor authentication. Authentication through verification of at least two of the following types of authentication factors:

a. Knowledge factors, such as a password.

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

c. Inherence factors, such as a biometric characteristic.

(11) Nonpublic information.

Electronic information that is not publicly available information and is any of the following:

a. Any information concerning a consumer which because of name, number, personal mark, or other identifier can be used to identify the consumer, in combination with any one or more of the following data elements:

1. The Social Security number.

2. The driver's license number or nondriver identification card number.

3. Any financial account number or a credit or debit card number.

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

5. Biometric records.

b. 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 can be used to identify a particular consumer, and that relates to any of the following:

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

2. The provision of health care to any consumer.

3. Payment for the provision of health care to any consumer.

(12) Person. Any individual or any nongovernmental entity, including, but not limited to, any nongovernmental partnership, corporation, branch, agency, or association.

(13)

a. Publicly available information. Any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from federal, state, or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state, or local law.

b. For the 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 both of the following:

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

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

(14) Risk assessment. The risk assessment that each licensee is required to conduct under subsection (c) of Section 27-62-4.

(15) State. The State of Alabama.

(16) Third-party service provider. A person, not defined as a licensee, who contracts with a licensee to maintain, process, store, or access nonpublic information through the provision of services to the licensee.

History

Acts 2019, No. 19-98, § 3, effective May 1, 2019.

Code of Ala. § 27-62-2

Current through the end of the 2023 First Special, Regular, and Second Special Sessions, but not including corrections and changes made to the 2023 session laws by the Code Commissioner.

Michie's™ Alabama Code > TITLE 27 Insurance (Chs. 1 — 64) > CHAPTER 62 Insurance Data Security Law (§§ 27-62-1 — 27-62-11)

§ 27-62-2. Purpose and intent.

(a) Notwithstanding any other provision of law, this chapter establishes the exclusive state standards applicable to licensees for data security, the investigation of a cybersecurity event as defined in Section 27-62-3, and notification to the Commissioner of Insurance of a cybersecurity event as provided by this chapter.

(b) This chapter may not be construed to create or imply a private cause of action for a violation of this chapter nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this chapter.

History

Acts 2019, No. 19-98, § 2, May 1, 2019.