Arkansas Code
Title 4 – Business and Commercial Law
Subtitle 7 – Consumer Protection
Chapter 110 – Personal Information Protection Act

4-110-101. Short title. This chapter shall be known and cited as the "Personal Information Protection Act".

4-110-102. Findings and purpose.
(a) It is the intent of the General Assembly to ensure that sensitive personal information about Arkansas residents is protected.

(b) To that end, the purpose of this chapter is to encourage individuals, businesses, and state agencies that acquire, own, or license personal information about the citizens of the State of Arkansas to provide reasonable security for the information.

4-110-103. Definitions. As used in this chapter:

(1) (A) "Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person or business.

(B) "Breach of the security of the system" does not include the good faith acquisition of personal information by an employee or agent of the person or business for the legitimate purposes of the person or business if the personal information is not otherwise used or subject to further unauthorized disclosure;

(2) (A) "Business" means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or of any other country or the parent or the subsidiary of a financial institution.

(B) "Business" includes:

(i) An entity that destroys records; and

(ii) A state agency;

(3) "Customer" means an individual who provides personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business;

(4) "Individual" means a natural person;

(5) "Medical information" means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional;

(6) "Owns or licenses" includes, but is not limited to, personal information that a business retains as part of the internal customer account of the business or for the purpose of using the information in transactions with the person to whom the information relates;

(7) "Personal information" means an individual's first name or first initial and his or her last name in combination with any one (1) or more of the following data elements when either the name or the data element is not encrypted or redacted:

(A) Social security number;

(B) Driver's license number or Arkansas identification card number;

(C) Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; and

(D) Medical information;

(8) (A) "Records" means any material that contains sensitive personal information in electronic form.

(B) "Records" does not include any publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number; and

(9) "State agencies" or "state agency" means any agency, institution, authority, department, board, commission, bureau, council, or other agency of the State of Arkansas supported by cash funds or the appropriation of state or federal funds.

4-110-104. Protection of personal information.

(a) A person or business shall take all reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information that is no longer to be retained by the person or business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.

(b) A person or business that acquires, owns, or licenses personal information about an Arkansas resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

4-110-105. Disclosure of security breaches.

(a) (1) Any person or business that acquires, owns, or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of Arkansas whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(2) The disclosure shall be made in the most expedient time and manner possible and without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in subsection (c) of this section, or any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) (1) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation.

(2) The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Notification under this section is not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers.

(e) For purposes of this section, notice may be provided by one (1) of the following methods:

(1) Written notice;

(2) Electronic mail notice if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001, as it existed on January 1, 2005; or

(3) (A) Substitute notice if the person or business demonstrates that:

(i) The cost of providing notice would exceed two hundred fifty thousand dollars ($250,000);

(ii) The affected class of persons to be notified exceeds five hundred thousand (500,000); or

(iii) The person or business does not have sufficient contact information.

(B) Substitute notice shall consist of all of the following:

(i) Electronic mail notice when the person or business has an electronic mail address for the subject persons;

(ii) Conspicuous posting of the notice on the website of the person or business if the person or business maintains a website; and

(iii) Notification by statewide media.

(f) Notwithstanding subsection (e) of this section, a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies affected persons in accordance with its policies in the event of a breach of the security of the system.

4-110-106. Exemptions.

(a) (1) The provisions of this chapter do not apply to a person or business that is regulated by a state or federal law that provides greater protection to personal information and at least as thorough disclosure requirements for breaches of the security of personal information than that provided by this chapter.

(2) Compliance with the state or federal law shall be deemed compliance with this chapter with regard to the subjects covered by this chapter.

(b) This section does not relieve a person or business from a duty to comply with any other requirements of other state and federal law regarding the protection and privacy of personal information.

4-110-107. Waiver. Any waiver of a provision of this chapter is contrary to public policy, void, and unenforceable.

4-110-108. Penalties. Any violation of this chapter is punishable by action of the Attorney General under the provisions of § 4-88-101 et seq.