[CHAPTER 487R]
DESTRUCTION OF PERSONAL INFORMATION RECORDS

Section

Note

Personal information protection requirements. L Sp 2008, c 10, §§7 to 15.

Cross References

Information privacy and security council; personal information security, see §§487N-5 to 7.

Personal information policy and oversight responsibilities for government agencies, see §487J-5.

" **§487R-1 Definitions.** As used in this chapter:

"Business" means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit. Except as provided in section 487R-2(e), the term includes a financial institution organized, chartered, or holding a license or authorization certificate under the laws of the State, any other state, the United States, or any other country, or the parent or the subsidiary of any such financial institution. The term also includes an entity whose business is records destruction.

"Disposal" means the discarding or abandonment of records containing personal information or the sale, donation, discarding, or transfer of any medium, including computer equipment or computer media, containing records of personal information, or other nonpaper media upon which records of personal information are stored, or other equipment for nonpaper storage of information.

"Government agency" means any department, division, board, commission, public corporation, or other agency or instrumentality of the State or any county.

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number;

(2) Driver's license number or Hawaii identification card number; or

(3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.

"Personal information" shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. "Encrypted", as used in this definition means the use of an algorithmic process to transform data into a form in which the

data is rendered unreadable or unusable without the use of a confidential process or key.

"Records" means any material on which written, drawn, spoken, visual, or electromagnetic information is recorded or preserved, regardless of physical form or characteristics. [L 2006, c 136, pt of §2; am L 2008, c 19, §71]

" **§487R-2 Destruction of personal information records.** (a) Any business or government agency that conducts business in Hawaii and any business or government agency that maintains or otherwise possesses personal information of a resident of Hawaii shall take reasonable measures to protect against unauthorized access to or use of the information in connection with or after its disposal.

(b) The reasonable measures shall include:

(1) Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, recycling, or shredding of papers containing personal information so that information cannot be practicably read or reconstructed;

(2) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media and other nonpaper media containing personal information so that the information cannot practicably be read or reconstructed; and

(3) Describing procedures relating to the adequate destruction or proper disposal of personal records as official policy in the writings of the business entity.

(c) A business or government agency may satisfy its obligation hereunder by exercising due diligence and entering into a written contract with, and thereafter monitoring compliance by, another party engaged in the business of records destruction to destroy personal information in a manner consistent with this section. Due diligence should ordinarily include one or more of the following:

(1) Reviewing an independent audit of the disposal business' operations or its compliance with this chapter;

(2) Obtaining information about the disposal business from several references or other reliable sources and requiring that the disposal business be certified by a recognized trade association or similar third party with a reputation for high standards of quality review; or

(3) Reviewing and evaluating the disposal business' information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the disposal business.

(d) A disposal business that conducts business in Hawaii or disposes of personal information of residents of Hawaii shall take reasonable measures to dispose of records containing personal information by implementing and monitoring compliance with policies and procedures that protect against unauthorized access to, or use of, personal information during or after the collection, transportation, and disposing of such information.

(e) This chapter shall not apply to any of the following:

(1) Any financial institution that is subject to 15 U.S.C. sections 6801 to 6809, as amended;

(2) Any health plan or healthcare provider that is subject to and in compliance with the standards for privacy of individually identifiable health information and the security standards for the protection of electronic health information of the Health Insurance Portability and Accountability Act of 1996; or

(3) Any consumer reporting agency that is subject to and in compliance with the Fair Credit Reporting Act, 15 U.S.C. sections 1681 to 1681x. [L 2006, c 136, pt of §2; am L 2008, c 19, §72]

" **[§487R-3] Penalties; civil action.** (a) Any business that violates any provision of this chapter shall be subject to penalties of not more than $2,500 for each violation. The attorney general or the executive director of the office of consumer protection may bring an action pursuant to this section. No such action may be brought against a government agency.

(b) In addition to any penalty provided for in subsection (a), any business that violates any provision of this chapter shall be liable to the injured party in an amount equal to the sum of any actual damages sustained by the injured party as a result of the violation. The court in any action brought under this section may award reasonable attorneys' fees to the prevailing party. No such action may be brought against a government agency.

(c) The penalties provided in this section shall be cumulative to the remedies or penalties available under all other laws of this State. [L 2006, c 136, pt of §2]

" **[§487R-4] Reporting requirements.** A government agency shall submit a written report to the legislature within twenty days after the discovery of a material occurrence of

unauthorized access to personal information records in connection with or after its disposal by or on behalf of the government agency. The report shall contain information relating to the nature of the incident, the number of individuals affected by the incident, and any procedures that have been implemented to prevent the incident from reoccurring. In the event that a law enforcement agency informs the government agency that the report may impede a criminal investigation or jeopardize national security, the report to the legislature may be delayed until twenty days after the law enforcement agency has determined that the report will no longer impede the investigation or jeopardize national security. [L 2006, c 136, pt of §2]