STATE OF NEBRASKA

SELECT INFORMATION TECHNOLOGY RELATED STATUTES

Table of Contents

48-3501. Act, how cited.

Sections 48-3501 to 48-3511 shall be known and may be cited as the Workplace Privacy Act.

Source: Laws 2016, LB821, § 1.

48-3502. Terms, defined.

For purposes of the Workplace Privacy Act:

(1) Adverse action means the discharge of an employee, a threat against an employee, or any other act against an employee that negatively affects the employee's employment;

(2) Applicant means a prospective employee applying for employment;

(3) Electronic communication device means a cellular telephone, personal digital assistant, electronic device with mobile data access, laptop computer, pager, broadband personal communication device, two-way messaging device, electronic game, or portable computing device;

(4) Employee means an individual employed by an employer;

(5) Employer means a public or nonpublic entity or an individual engaged in a business, an industry, a profession, a trade, or other enterprise in the state, including any agent, representative, or designee acting directly or indirectly in the interest of such an employer; and

(6)(a) Personal Internet account means an individual's online account that requires login information in order to access or control the account.

(b) Personal Internet account does not include:

(i) An online account that an employer or educational institution supplies or pays for, except when the employer or educational institution pays only for additional features or enhancements to the online account; or

(ii) An online account that is used exclusively for a business purpose of the employer.

Source: Laws 2016, LB821, § 2.

48-3503. Employer; prohibited acts.

No employer shall:

(1) Require or request that an employee or applicant provide or disclose any user name or password or any other related account information in order to gain access to the employee's or applicant's personal Internet account by way of an electronic communication device;

(2) Require or request that an employee or applicant log into a personal Internet account by way of an electronic communication device in the presence of the employer in a manner that enables the employer to observe the contents of the employee's or applicant's personal Internet account or provides the employer access to the employee's or applicant's personal Internet account;

(3) Require an employee or applicant to add anyone, including the employer, to the list of contacts associated with the employee's or applicant's personal Internet account or require or otherwise coerce an employee or applicant to change the settings on the employee's or applicant's personal Internet account which affects the ability of others to view the content of such account; or

(4) Take adverse action against, fail to hire, or otherwise penalize an employee or applicant for failure to provide or disclose any of the information or to take any of the actions specified in subdivisions (1) through (3) of this section.

Source: Laws 2016, LB821, § 3.

48-3504. Waiver of right or protection under act prohibited.

An employer shall not require an employee or applicant to waive or limit any protection granted under the Workplace Privacy Act as a condition of continued employment or of applying for or receiving an offer of employment. Any agreement to waive any right or protection under the act is against the public policy of this state and is void and unenforceable.

Source: Laws 2016, LB821, § 4.

48-3505. Retaliation or discrimination.

An employer shall not retaliate or discriminate against an employee or applicant because the employee or applicant:

(1) Files a complaint under the Workplace Privacy Act; or

(2) Testifies, assists, or participates in an investigation, proceeding, or action concerning a violation of the act.

Source: Laws 2016, LB821, § 5.

48-3506. Employee acts prohibited.

An employee shall not download or transfer an employer's private proprietary information or private financial data to a personal Internet account without authorization from the employer.

This section shall not apply if the proprietary information or the financial data is otherwise disclosed by the employer to the public pursuant to other provisions of law or practice.

Source: Laws 2016, LB821, § 6.

48-3507. Employer's rights not limited by act.

Nothing in the Workplace Privacy Act limits an employer's right to:

(1) Promulgate and maintain lawful workplace policies governing the use of the employer's electronic equipment, including policies regarding Internet use and personal Internet account use;

(2) Request or require an employee or applicant to disclose access information to the employer to gain access to or operate:

(a) An electronic communication device supplied by or paid for in whole or in part by the employer; or

(b) An account or service provided by the employer, obtained by virtue of the employee's employment relationship with the employer, or used for the employer's business purposes;

(3) Restrict or prohibit an employee’s access to certain web sites while using an electronic communication device supplied by or paid for in whole or in part by the employer or while using an employer’s network or resources, to the extent permissible under applicable laws;

(4) Monitor, review, access, or block electronic data stored on an electronic communication device supplied by or paid for in whole or in part by the employer or stored on an employer’s network, to the extent permissible under applicable laws;

(5) Access information about an employee or applicant that is in the public domain or is otherwise obtained in compliance with the Workplace Privacy Act;

(6) Conduct an investigation or require an employee to cooperate in an investigation under any of the following circumstances:

(a) If the employer has specific information about potentially wrongful activity taking place on the employee’s personal Internet account, for the purpose of ensuring compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct; or

(b) If the employer has specific information about an unauthorized download or transfer of the employer's private proprietary information, private financial data, or other confidential information to an employee’s personal Internet account;

(7) Take adverse action against an employee for downloading or transferring an employer's private proprietary information or private financial data to a personal Internet account without the employer's authorization;

(8) Comply with requirements to screen employees or applicants before hiring or to monitor or retain employee communications that are established by state or federal law or by a self-regulatory organization as defined in 15 U.S.C. 78c(a)(26), as such section existed on January 1, 2016; or

(9) Comply with a law enforcement investigation conducted by a law enforcement agency.

Source: Laws 2016, LB821, § 7.

48-3508. Law enforcement agency rights.

Nothing in the Workplace Privacy Act limits a law enforcement agency's right to screen employees or applicants in connection with a law enforcement employment application or a law enforcement officer conduct investigation.

Source: Laws 2016, LB821, § 8.

48-3509. Personal Internet account; employer; duty; liability.

(1) The Workplace Privacy Act does not create a duty for an employer to search or monitor the activity of a personal Internet account.

(2) An employer is not liable under the act for failure to request or require that an employee or applicant grant access to, allow observation of, or disclose information that allows access to or observation of the employee's or applicant's personal Internet account.

Source: Laws 2016, LB821, § 9.

48-3510. Employer; limit on liability and use of certain information.

If an employer inadvertently learns the user name, password, or other means of access to an employee's or applicant's personal Internet account through the use of otherwise lawful technology that monitors the employer's computer network or employer-provided electronic communication devices for service quality or security purposes, the employer is not liable for obtaining the information, but the employer shall not use the information to access the employee's or applicant's personal Internet account or share the information with anyone. The employer shall delete such information as soon as practicable.

Source: Laws 2016, LB821, § 10.

48-3511. Civil action authorized.

Upon violation of the Workplace Privacy Act, an aggrieved employee or applicant may, in addition to any other available remedy, institute a civil action within one year after the date of the alleged violation or the discovery of the alleged violation, whichever is later. The employee or applicant shall file an action directly in the district court of the county where such alleged violation occurred. The district court shall file and try such case as any other civil action, and any successful complainant shall be entitled to appropriate relief, including temporary or permanent injunctive relief, general and special damages, reasonable attorney's fees, and costs.

Source: Laws 2016, LB821, § 11; Laws 2018, LB193, § 85.

Operative Date: July 19, 2018

Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006

87-801. Act, how cited.

Sections 87-801 to 87-808 shall be known and may be cited as the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006.

Source: Laws 2006, LB 876, § 1; Laws 2018, LB757, § 6.
Effective Date: July 19, 2018

87-802. Terms, defined.

For purposes of the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006:

(1) Breach of the security of the system means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by an individual or a commercial entity. Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system if the personal information is not used or subject to further unauthorized disclosure. Acquisition of personal information pursuant to a search warrant, subpoena, or other court order or pursuant to a subpoena or order of a state agency is not a breach of the security of the system;

(2) Commercial entity includes a corporation, business trust, estate, trust, partnership, limited partnership, limited liability partnership, limited liability company, association, organization, joint venture, government, governmental subdivision, agency, or instrumentality, or any other legal entity, whether for profit or not for profit;

(3) Encrypted means converted by use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key. Data shall not be considered encrypted if the confidential process or key was or is reasonably believed to have been acquired as a result of the breach of the security of the system;

(4) Notice means:

(a) Written notice;

(b) Telephonic notice;

(c) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001, as such section existed on January 1, 2006;

(d) Substitute notice, if the individual or commercial entity required to provide notice demonstrates that the cost of providing notice will exceed seventy-five thousand dollars, that the affected class of Nebraska residents to be notified exceeds one hundred thousand residents, or that the individual or commercial entity does not have sufficient contact information to provide notice. Substitute notice under this subdivision requires all of the following:

(i) Electronic mail notice if the individual or commercial entity has electronic mail addresses for the members of the affected class of Nebraska residents;

(ii) Conspicuous posting of the notice on the web site of the individual or commercial entity if the individual or commercial entity maintains a web site; and

(iii) Notice to major statewide media outlets; or

(e) Substitute notice, if the individual or commercial entity required to provide notice has ten employees or fewer and demonstrates that the cost of providing notice will exceed ten thousand dollars. Substitute notice under this subdivision requires all of the following:

(i) Electronic mail notice if the individual or commercial entity has electronic mail addresses for the members of the affected class of Nebraska residents;

(ii) Notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the individual or commercial entity is located, which advertisement shall be of sufficient size that it covers at least one-quarter of a page in the newspaper and shall be published in the newspaper at least once a week for three consecutive weeks;

(iii) Conspicuous posting of the notice on the web site of the individual or commercial entity if the individual or commercial entity maintains a web site; and

(iv) Notification to major media outlets in the geographic area in which the individual or commercial entity is located;

(5) Personal information means either of the following:

(a) A Nebraska resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident if either the name or the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable:

(i) Social security number;

(ii) Motor vehicle operator's license number or state identification card number;

(iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account;

(iv) Unique electronic identification number or routing code, in combination with any required security code, access code, or password; or

(v) Unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation; or

(b) A user name or email address, in combination with a password or security question and answer, that would permit access to an online account.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records; and

(6) Redact means to alter or truncate data such that no more than the last four digits of a social security number, motor vehicle operator's license number, state identification card number, or account number is accessible as part of the personal information.

Source: Laws 2006, LB 876, § 2; Laws 2016, LB835, § 27.

87-803. Breach of security; investigation; notice to resident; notice to Attorney General.

(1) An individual or a commercial entity that conducts business in Nebraska and that owns or licenses computerized data that includes personal information about a resident of Nebraska shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be used for an unauthorized purpose. If the investigation determines that the use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur, the individual or commercial entity shall give notice to the affected Nebraska resident. Notice shall be made as soon as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

(2) If notice of a breach of security of the system is required by subsection (1) of this section, the individual or commercial entity shall also, not later than the time when notice is provided to the Nebraska resident, provide notice of the breach of security of the system to the Attorney General.

(3) An individual or a commercial entity that maintains computerized data that includes personal information that the individual or commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system when it becomes aware of a breach if use of personal information about a Nebraska resident for an unauthorized purpose occurred or is reasonably likely to occur. Cooperation includes, but is not limited to, sharing with the owner or licensee information relevant to the breach, not including information proprietary to the individual or commercial entity.

(4) Notice required by this section may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice shall be made in good faith, without unreasonable delay, and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.

Source: Laws 2006, LB 876, § 3; Laws 2016, LB835, § 28.

87-804. Compliance with notice requirements; manner.

(1) An individual or a commercial entity that maintains its own notice procedures which are part of an information security policy for the treatment of personal information and which are otherwise consistent with the timing requirements of section 87-803, is deemed to be in compliance with the notice requirements of section 87-803 if the individual or the commercial entity notifies affected Nebraska residents and the Attorney General in accordance with its notice procedures in the event of a breach of the security of the system.

(2) An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with section 87-803 if the individual or commercial entity notifies affected Nebraska residents and the Attorney General in accordance with the maintained procedures in the event of a breach of the security of the system.

Source: Laws 2006, LB 876, § 4; Laws 2016, LB835, § 29.

87-805. Waiver; void and unenforceable.

Any waiver of the provisions of the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006 is contrary to public policy and is void and unenforceable.

Source: Laws 2006, LB 876, § 5.

87-806. Attorney General; powers; violation; how treated.

(1) For purposes of the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, the Attorney General may issue subpoenas and seek and recover direct economic damages for each affected Nebraska resident injured by a violation of section 87-803.

(2) A violation of section 87-808 shall be considered a violation of section 59-1602 and be subject to the Consumer Protection Act and any other law which provides for the implementation and enforcement of section 59-1602. A violation of section 87-808 does not give rise to a private cause of action.

Source: Laws 2006, LB 876, § 6; Laws 2018, LB757, § 8.
Effective Date: July 19, 2018

87-807. Act; applicability.

The Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006 applies to the discovery of or notification pertaining to a breach of the security of the system that occurs on or after July 14, 2006.

Source: Laws 2006, LB 876, § 7.

87-808. Security procedures and practices; disclosure of computerized data; contract provisions; compliance.

(1) To protect personal information from unauthorized access, acquisition, destruction, use, modification, or disclosure, an individual or a commercial entity that conducts business in Nebraska and owns, licenses, or maintains computerized data that includes personal information about a resident of Nebraska shall implement and maintain reasonable security procedures and practices that are appropriate to the nature and sensitivity of the personal information owned, licensed, or maintained and the nature and size of, and the resources available to, the business and its operations, including safeguards that protect the personal information when the individual or commercial entity disposes of the personal information.

(2)(a) An individual or commercial entity that discloses computerized data that includes personal information about a Nebraska resident to a nonaffiliated, third-party service provider shall require by contract that the service provider implement and maintain reasonable security procedures and practices that:

(i) Are appropriate to the nature of the personal information disclosed to the service provider; and

(ii) Are reasonably designed to help protect the personal information from unauthorized access, acquisition, destruction, use, modification, or disclosure.

(b) This subsection does not apply to any contract entered into before July 19, 2018. Any such contract renewed on or after July 19, 2018, shall comply with the requirements of this subsection.

(3) An individual or a commercial entity complies with subsections (1) and (2) of this section if the individual or commercial entity:

(a) Complies with a state or federal law that provides greater protection to personal information than the protections that this section provides; or

(b) Complies with the regulations promulgated under Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801 et seq., or the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. 1320d to 1320d-9, as such acts and sections existed on January 1, 2018, if the individual or commercial entity is subject to either or both of such acts or sections.

Source: Laws 2018, LB757, § 7.

Effective Date: July 19, 2018

--

Sources:

- Workplace Privacy Act: http://nebraskalegislature.gov/laws/display_html.php?begin_section=48-3501&end_section=48-3511
- Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006: http://nebraskalegislature.gov/laws/display_html.php?begin_section=87-801&end_section=87-808

Date: July 2018