Information Breach Notification and Cloud Providers

The Act requires that in the event of a data security breach information holders are to contact anyone whose data may have been accessed by an unauthorized person. Additionally, this Act requires that cloud computing service providers will not process student data without parental permission.

Submitted as:
Kentucky
HB 232
Status: Signed into law on April 10, 2014.

Suggested State Legislation

(Title, enacting clause, etc.)

Section 1. [*Security breach notifications*.]

(1) As used in this section, unless the context otherwise requires:

(a) "Breach of the security of the system" means unauthorized acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of personally identifiable information maintained by the information holder as part of a database regarding multiple individuals that actually causes, or leads the information holder to reasonably believe has caused or will cause, identity theft or fraud against any resident of the [Commonwealth of Kentucky]. Good faith acquisition of personally identifiable information by an employee or agent of the information holder for the purposes of the information holder is not a breach of the security of the system if the personally identifiable information is not used or subject to further unauthorized disclosure;

(b) "Information holder" means any person or business entity that conducts business in this state; and

(c) "Personally identifiable information" means an individual's first name or first initial and last name in combination with any one (1) or more of the following data elements, when the name or data element is not redacted:

1. Social Security number;
2. Driver's license number; or
3. Account number, credit or debit card number, in combination with any required security code, access code, or password permit access to an individual's financial account.

(2) Any information holder shall disclose any breach of the security of the system, following discovery or notification of the breach in the security of the data, to any resident of [Kentucky] whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (4) of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(3) Any information holder that maintains computerized data that includes personally identifiable information that the information holder does not own shall notify the owner or licensee of the information of any breach of the security of the data as soon as reasonably practicable following discovery, if the personally identifiable information was, or is reasonably believed to have been, acquired by an unauthorized person.

(4) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.

(5) For purposes of this section, notice may be provided by one (1) of the following methods:
   (a) Written notice;
   (b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. sec. 7001; or
   (c) Substitute notice, if the information holder demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds five hundred thousand (500,000), or the information holder does not have sufficient contact information. Substitute notice shall consist of all of the following:
      1. E-mail notice, when the information holder has an e-mail address for the subject persons;
      2. Conspicuous posting of the notice on the information holder's Internet Web site page, if the information holder maintains a Web site page; and
      3. Notification to major statewide media.

(6) Notwithstanding subsection (5) of this section, an information holder that maintains its own notification procedures as part of an information security policy for the treatment of personally identifiable 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 it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(7) If a person discovers circumstances requiring notification pursuant to this section of more than one thousand (1,000) persons at one (1) time, the person shall also notify, without unreasonable delay, all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. sec. 1681a, of the timing, distribution, and content of the notices.

(8) The provisions of this section and the requirements for nonaffiliated third parties in [Insert citation] shall not apply to any person who is subject to the provisions of Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, as amended, or the federal Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, as amended, or any agency of the [Commonwealth of Kentucky] or any of its local governments or political subdivisions.

Section 2. [*Student data; cloud computing services*.]

(1) As used in this section:
   (a) “Cloud computing service” means a service that provides, and that is marketed and designed to provide, an educational institution with account-based access to online computing resources;

(b) “Cloud computing service provider” means any person other than an educational institution that operates a cloud computing service;
(c) “Educational institution” means any public, private, or school administrative unit serving students in kindergarten to grade twelve (12);
(d) “Person” means an individual, partnership, corporation, association, company, or any other legal entity;
(e) “Process” means to use, access, collect, manipulate, scan, modify, analyze, transform, disclose, store, transmit, aggregate, or dispose of student data;
(f) “Student data” means any information or material, in any medium or format, that concerns a student and is created or provided by the student in the course of the student's use of cloud computing services, or by an agent or employee of the educational institution in connection with the cloud computing services. Student data includes the student's name, email address, email messages, postal address, phone number, and any documents, photos, or unique identifiers relating to the student.

(2) A cloud computing service provider shall not process student data for any purpose other than providing, improving, developing, or maintaining the integrity of its cloud computing services, unless the provider receives express permission from the student's parent. However, a cloud computing service provider may assist an educational institution to conduct educational research as permitted by the Family Educational Rights and Privacy Act of 1974, as amended, 20 U.S.C. sec. 1232g. A cloud computing service provider shall not in any case process student data to advertise or facilitate advertising or to create or correct an individual or household profile for any advertisement purpose, and shall not sell, disclose, or otherwise process student data for any commercial purpose.

(3) A cloud computing service provider that enters into an agreement to provide cloud computing services to an educational institution shall certify in writing to the educational institution that it will comply with subsection (2) of this section.

(4) The [Kentucky] Board of Education may promulgate administrative regulations as necessary to carry out the requirements of this section.