365.720 Definitions for KRS 365.720 to 365.730.

As used in KRS 365.720 to 365.730, unless the context requires otherwise:

(1) "Business" means a sole proprietorship, partnership, corporation, limited liability company, association, or other entity, however organized and whether or not organized to operate at a profit. "Business" shall not mean a bank as defined in 12 U.S.C. sec. 1813(a) or Subtitles 1, 2, and 3 of KRS Chapter 286, a credit union as defined in 12 U.S.C. sec. 1752 or Subtitle 6 of KRS Chapter 286, a savings association as defined in 12 U.S.C. sec. 1813(b), or an association as defined in Subtitle 5 of KRS Chapter 286. The term includes an entity that destroys records;

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

(3) "Individual" means a natural person;

(4) "Personally identifiable information" means data capable of being associated with a particular customer through one (1) or more identifiers, including but not limited to a customer's name, address, telephone number, electronic mail address, fingerprints, photographs or computerized image, Social Security number, passport number, driver identification number, personal identification card number or code, date of birth, medical information, financial information, tax information, and disability information; and

(5) "Records" means any material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed, or electromagnetically transmitted.

Effective: July 12, 2006

History: Created 2006 Ky. Acts ch. 42, sec. 4, effective July 12, 2006.

365.725 Destruction of customer's records containing personally identifiable information.

When a business disposes of, other than by storage, any customer's records that are not required to be retained, the business shall take reasonable steps to destroy, or arrange for the destruction of, that portion of the records containing personally identifiable information by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or indecipherable through any means.

Effective: July 12, 2006

History: Created 2006 Ky. Acts ch. 42, sec. 5, effective July 12, 2006.

365.730 Civil action for damages or injunction for violation of KRS 365.725 -- Rights and remedies.

(1) Any customer injured by a violation of KRS 365.725 may institute a civil action to recover damages.

(2) Any business that violates, proposes to violate, or has violated any provision of KRS 365.725 may be enjoined in a civil action.

(3) The rights and remedies available under this section shall be cumulative to each other and to any other rights and remedies available under law.

Effective: July 12, 2006

History: Created 2006 Ky. Acts ch. 42, sec. 6, effective July 12, 2006.

365.732 Notification to affected persons of computer security breach involving their unencrypted personally identifiable information.

(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 or credit or debit card number, in combination with any required security code, access code, or password to 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 KRS Chapter 61 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.

Effective: July 15, 2014

History: Created 2014 Ky. Acts ch. 84, sec. 1, effective July 15, 2014.

365.734 Prohibited uses of personally identifiable student information by cloud computing service provider -- Administrative regulations.

(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; and

(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, e-mail address, e-mail 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 in accordance with KRS Chapter 13A as necessary to carry out the requirements of this section.

Effective: July 15, 2014

History: Created 2014 Ky. Acts ch. 84, sec. 2, effective July 15, 2014.