13.055 DISCLOSURE OF BREACH IN SECURITY; NOTIFICATION AND INVESTIGATION REPORT REQUIRED.

Subdivision 1. **Definitions.** For purposes of this section, the following terms have the meanings given to them.

(a) "Breach of the security of the data" means unauthorized acquisition of data maintained by a government entity that compromises the security and classification of the data. Good faith acquisition of or access to government data by an employee, contractor, or agent of a government entity for the purposes of the entity is not a breach of the security of the data, if the government data is not provided to or viewable by an unauthorized person, or accessed for a purpose not described in the procedures required by section 13.05, subdivision 5. For purposes of this paragraph, data maintained by a government entity includes data maintained by a person under a contract with the government entity that provides for the acquisition of or access to the data by an employee, contractor, or agent of the government entity.

(b) "Contact information" means either name and mailing address or name and e-mail address for each individual who is the subject of data maintained by the government entity.

(c) "Unauthorized acquisition" means that a person has obtained, accessed, or viewed government data without the informed consent of the individuals who are the subjects of the data or statutory authority and with the intent to use the data for nongovernmental purposes.

(d) "Unauthorized person" means any person who accesses government data without a work assignment that reasonably requires access, or regardless of the person's work assignment, for a purpose not described in the procedures required by section 13.05, subdivision 5.

Subd. 2. **Notice to individuals; investigation report.** (a) A government entity that collects, creates, receives, maintains, or disseminates private or confidential data on individuals must disclose any breach of the security of the data following discovery or notification of the breach. Written notification must be made to any individual who is the subject of the data and whose private or confidential data was, or is reasonably believed to have been, acquired by an unauthorized person and must inform the individual that a report will be prepared under paragraph (b), how the individual may obtain access to the report, and that the individual may request delivery of the report by mail or e-mail. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with (1) the legitimate needs of a law enforcement agency as provided in subdivision 3; or (2) any measures necessary to determine the scope of the breach and restore the reasonable security of the data.

(b) Notwithstanding section 13.15 or 13.37, upon completion of an investigation into any breach in the security of data and final disposition of any disciplinary action for purposes of section 13.43, including exhaustion of all rights of appeal under any applicable collective bargaining agreement, the responsible authority shall prepare a report on the facts and results of the investigation. If the breach involves unauthorized access to or acquisition of data by an employee, contractor, or agent of the government entity, the report must at a minimum include:

(1) a description of the type of data that were accessed or acquired;

(2) the number of individuals whose data was improperly accessed or acquired;

(3) if there has been final disposition of disciplinary action for purposes of section 13.43, the name of each employee determined to be responsible for the unauthorized access or acquisition, unless the employee was performing duties under chapter 5B; and

(4) the final disposition of any disciplinary action taken against each employee in response.

Subd. 3. **Delayed notice.** The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede an active criminal investigation. The notification required by this section must be made after the law enforcement agency determines that it will not compromise the investigation.

Subd. 4. **Method of notice.** Notice under this section may be provided by one of the following methods:

(a) written notice by first class mail to each affected individual;

(b) electronic notice to each affected individual, if the notice provided is consistent with the provisions regarding electronic records and signatures as set forth in United States Code, title 15, section 7001; or

(c) substitute notice, if the government entity demonstrates that the cost of providing the written notice required by paragraph (a) would exceed $250,000, or that the affected class of individuals to be notified exceeds 500,000, or the government entity does not have sufficient contact information. Substitute notice consists of all of the following:

(i) e-mail notice if the government entity has an e-mail address for the affected individuals;

(ii) conspicuous posting of the notice on the website page of the government entity, if the government entity maintains a website; and

(iii) notification to major media outlets that reach the general public within the government entity's jurisdiction.

Subd. 5. **Coordination with consumer reporting agencies.** If the government entity discovers circumstances requiring notification under this section of more than 1,000 individuals at one time, the government entity must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in United States Code, title 15, section 1681a, of the timing, distribution, and content of the notices.

Subd. 6. **Security assessments.** At least annually, each government entity shall conduct a comprehensive security assessment of any personal information maintained by the government entity. For the purposes of this subdivision, personal information is defined under section 325E.61, subdivision 1, paragraphs (e) and (f).

Subd. 7. **Access to data for audit purposes.** Nothing in this section or section 13.05, subdivision 5, restricts access to not public data by the legislative auditor or state auditor in the performance of official duties.

History: *2005 c 163 s 21; 2005 c 167 s 1; 2006 c 212 art 1 s 17,24; 2006 c 233 s 7,8; 2014 c 284 s 2*