Section 1. Minnesota Statutes 2012, section 13.05, subdivision 5, is amended to read:

Subd. 5. **Data protection.** (a) The responsible authority shall:

(1) establish procedures to assure that all data on individuals is accurate, complete, and current for the purposes for which it was collected; ~~and~~

(2) establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that are not public are only accessible to persons whose work assignment reasonably requires access to the data, and is only being accessed by those persons for purposes described in the procedure; and

(3) develop a policy incorporating these procedures, which may include a model policy governing access to the data if sharing of the data with other government entities is authorized by law.

(b) When not public data is being disposed of, the data must be destroyed in a way that prevents its contents from being determined.

Sec. 2. Minnesota Statutes 2012, section 13.055, is amended to read:

**13.055 ~~STATE AGENCIES;~~ 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.

Section 1. **[13.026] INVENTORY OF SURVEILLANCE TECHNOLOGY.**

Subdivision 1. **Inventory required.** The responsible authority of a government entity shall prepare and update an inventory of surveillance technology maintained or used by the government entity. For purposes of this section, "surveillance technology" means technology that:

(1) can be used to track the location, personal characteristics, or activities of an individual or the property of an individual; or

(2) is a powered, aerial vehicle that does not carry a human operator; can fly autonomously or be piloted remotely; and can be expendable or recoverable.

Subd. 2. **Report.** By January 15 of each year, a government entity shall submit a report to the legislature that includes an inventory of all surveillance technologies maintained or used by the government entity during the previous calendar year and any new surveillance technology that the government entity may maintain or use during the current calendar year. The report must be submitted to the chairs and ranking minority members of the policy committees of the legislature with jurisdiction over data practices issues.

(a) "Breach of the security of the data" means unauthorized acquisition of or access to data maintained by a ~~state agency~~ 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 ~~state agency~~ government entity for the purposes of the ~~state agency~~ 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 ~~state agency~~ government entity.

(c) "Unauthorized acquisition" means that a person has obtained 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 permission or~~ without a work assignment that reasonably requires ~~the person to have~~ access ~~to the data~~, 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 ~~state agency~~ 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. 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) Upon completion of an investigation into any breach in the security of data, including exhaustion of all rights of appeal under any applicable collective bargaining agreement or other law, 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 data that were accessed or acquired; and

(2) if disciplinary action was taken against an employee:

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

(ii) the name of each employee determined responsible for the unauthorized access or acquisition; and

(iii) the final disposition of the disciplinary action taken against the employee in response.

(c) The report must not include data that are not public under other law.

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 ~~state agency~~ 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 ~~state agency~~ government entity does not have sufficient contact information. Substitute notice consists of all of the following:

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

(ii) conspicuous posting of the notice on the Web site page of the ~~state agency~~ government entity, if the ~~state agency~~ government entity maintains a Web site; 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 ~~state agency~~ government entity discovers circumstances requiring notification under this section of more than 1,000 individuals at one time, the ~~state agency~~ 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).

**EFFECTIVE DATE.** This section is effective August 1, 2013, and applies to security breaches occurring on or after that date.

Sec. 3. Minnesota Statutes 2012, section 13.09, is amended to read:

**13.09 PENALTIES.**

(a) Any person who willfully violates the provisions of this chapter or any rules adopted under this chapter or whose conduct constitutes the knowing unauthorized acquisition of not public data, as defined in section 13.055, subdivision 1, is guilty of a misdemeanor.

(b) Willful violation of this chapter ~~by~~, including any action subject to a criminal penalty under paragraph (a), by any public employee constitutes just cause for suspension without pay or dismissal of the public employee.

**EFFECTIVE DATE.** This section is effective August 1, 2013, and applies to crimes committed on or after that date.

Sec. 4. Minnesota Statutes 2012, section 13.82, is amended by adding a subdivision to read:

Subd. 31. **License plate reader data.** (a) For purposes of this subdivision, "automated license plate reader data" means government data derived from an automated reader that captures motor vehicle license plate numbers.

Sec. 2. Minnesota Statutes 2012, section 13.82, is amended by adding a subdivision to read:

Subd. 31. **Automated license plate reader.** (a) As used in this subdivision, "automated license plate reader" means an electronic device mounted on a law enforcement vehicle or positioned in a stationary location that is capable of recording data on, or taking a photograph of, a vehicle or its license plate and comparing the collected data and photographs to existing law enforcement databases for investigative purposes.

(b) Data collected by an automated license plate reader are confidential data on individuals or protected nonpublic data if the data are or become active criminal investigative data.

| | |
|---|---|
| (b) Automated license plate reader data are private data on individuals or nonpublic data. Notwithstanding section 138.17, automated license plate reader data must not be retained, in any format, unless, based on a search of the Minnesota license plate data file, the data identify a vehicle or license plate that has been stolen, there is a warrant for the arrest of the owner of the vehicle or the owner has a suspended or revoked driver's license, or the data are active investigative data. | (c) The following data collected by an automated license plate reader that are not classified under paragraph (b) are private data on individuals or nonpublic data:<br>(1) license plate numbers;<br>(2) date, time, and location data on vehicles; and<br>(3) pictures of license plates, vehicles, and areas surrounding the vehicles.<br>(d) Notwithstanding section 138.17, data collected by an automated license plate reader must be destroyed:<br>(1) 90 days from the time of collection, if the data are classified under paragraph (c); or<br>(2) upon request of a program participant under chapter 5B, at the time of collection or upon receipt of the request, whichever occurs later, unless the data are classified under paragraph (b).<br>Data on a request of a program participant under clause (2) are private data on individuals. If data collected by an automated license plate reader are shared with another law enforcement agency, the agency that receives the data must comply with the data destruction requirements of this paragraph. |
| (c) A law enforcement agency that installs or uses an automated license plate reader must maintain a log of its use, including: | (e) A law enforcement agency that installs or uses an automated license plate reader must maintain a log of its use, including: |
| (1) locations at which the reader is installed or used; | (1) specific times of day that the reader actively collected data; |
| (2) specific times of day that the reader actively collected data; and | (2) the aggregate number of vehicles or license plates on which data are collected for each period of active use; and |
| (3) the aggregate number of vehicles or license plates on which data are collected for each period of active use. | (3) for a reader at a stationary location, the location at which the reader actively collected data. |
| Notwithstanding any other law to the contrary, data contained in a log required under this paragraph are public. | Data in a log required under this paragraph are public. |
| (d) The responsible law enforcement agency shall conduct a biennial audit of data collected from automated license plate readers to determine whether the data has been classified or destroyed as required under this subdivision. Specific data used in the audit under this paragraph are classified as provided in paragraph (b). Summary data related to the results of the audit are public. | (f) In addition to the log required under paragraph (e), the law enforcement agency must maintain records showing the date the data were collected and whether the data are classified under paragraph (b) or (c). The Department of Public Safety shall conduct a biennial audit of the records to determine whether data currently in the records are classified and destroyed as required under this subdivision and to verify compliance with paragraph (g). Data in the records required under this paragraph are classified as provided in paragraph (b) or (c). Summary results of the audit are public. |

(e) A law enforcement agency may not use an automated license plate reader unless the agency has implemented policies and procedures necessary to ensure compliance with this subdivision.

Sec. 5. Minnesota Statutes 2012, section 299C.40, subdivision 4, is amended to read:

Subd. 4. **Data classification; general rule; changes in classification; audit trail.** (a) The classification of data in the law enforcement agency does not change after the data is submitted to CIBRS. If CIBRS is the only source of data made public by section 13.82, subdivisions 2, 3, 6, and 7, data described in those subdivisions must be downloaded and made available to the public as required by section 13.03.

(b) Data on individuals created, collected, received, maintained, or disseminated by CIBRS is classified as confidential data on individuals as defined in section 13.02, subdivision 3, and becomes private data on individuals as defined in section 13.02, subdivision 12, as provided by this section.

(c) Data not on individuals created, collected, received, maintained, or disseminated by CIBRS is classified as protected nonpublic data as defined in section 13.02, subdivision 13, and becomes nonpublic data as defined in section 13.02, subdivision 9, as provided by this section.

(d) Confidential or protected nonpublic data created, collected, received, maintained, or disseminated by CIBRS must automatically change classification from confidential data to private data or from protected nonpublic data to nonpublic data on the earlier of the following dates:

(g) A law enforcement agency must comply with sections 13.05, subdivision 5, and 13.055 in the operation of automated license plate readers and access to the data. The responsible authority for a law enforcement agency must establish written procedures to ensure that law enforcement personnel have access to the data only if authorized in writing by the chief of police, sheriff, or head of the law enforcement agency, or their designee, to obtain access to data collected by an automated license plate reader for a specific law enforcement purpose.

(h) Within ten days of the installation or current use of an automated license plate reader, a law enforcement agency must notify the Bureau of Criminal Apprehension of any fixed location of a stationary automated license plate reader and, if applicable, if the agency uses any other automated license plate reader. The Bureau of Criminal Apprehension must maintain a list of law enforcement agencies using automated license plate readers, including locations of any fixed stationary automated license plate readers, except to the extent that the location of the reader is security information, as defined in section 13.37. This list is accessible to the public and must be available on the bureau's Web site.

**EFFECTIVE DATE.** This section is effective the day following final enactment. Data collected before the effective date of this section must be destroyed, if required by this section, no later than 15 days after the date this section becomes effective.

(1) upon receipt by CIBRS of notice from a law enforcement agency that an investigation has become inactive; or

(2) when the data has not been updated by the law enforcement agency that submitted it for a period of 120 days.

(e) For the purposes of this section, an investigation becomes inactive upon the occurrence of any of the events listed in section 13.82, subdivision 7, clauses (a) to (c).

(f) Ten days before making a data classification change because data has not been updated, CIBRS must notify the law enforcement agency that submitted the data that a classification change will be made on the 120th day. The notification must inform the law enforcement agency that the data will retain its classification as confidential or protected nonpublic data if the law enforcement agency updates the data or notifies CIBRS that the investigation is still active before the 120th day. A new 120-day period begins if the data is updated or if a law enforcement agency notifies CIBRS that an active investigation is continuing.

(g) A law enforcement agency that submits data to CIBRS must notify CIBRS if an investigation has become inactive so that the data is classified as private data or nonpublic data. The law enforcement agency must provide this notice to CIBRS within ten days after an investigation becomes inactive.

(h) All queries and responses and all actions in which data is submitted to CIBRS, changes classification, or is disseminated by CIBRS to any law enforcement agency must be recorded in the CIBRS audit trail.

(i) Notwithstanding paragraphs (b) and (c), the name of each law enforcement agency that submits data to CIBRS, and a general description of the types of data submitted by the agency, are public.