13.82 COMPREHENSIVE LAW ENFORCEMENT DATA.

Subdivision 1. **Application.** This section shall apply to agencies which carry on a law enforcement function, including but not limited to municipal police departments, county sheriff departments, fire departments, the Bureau of Criminal Apprehension, the Minnesota State Patrol, the Board of Peace Officer Standards and Training, the Department of Commerce, and county human service agency client and provider fraud investigation, prevention, and control units operated or supervised by the Department of Human Services.

Subd. 2. **Arrest data.** The following data created or collected by law enforcement agencies which document any actions taken by them to cite, arrest, incarcerate or otherwise substantially deprive an adult individual of liberty shall be public at all times in the originating agency:

(a) time, date and place of the action;

(b) any resistance encountered by the agency;

(c) any pursuit engaged in by the agency;

(d) whether any weapons were used by the agency or other individual;

(e) the charge, arrest or search warrants, or other legal basis for the action;

(f) the identities of the agencies, units within the agencies and individual persons taking the action;

(g) whether and where the individual is being held in custody or is being incarcerated by the agency;

(h) the date, time and legal basis for any transfer of custody and the identity of the agency or person who received custody;

(i) the date, time and legal basis for any release from custody or incarceration;

(j) the name, age, sex and last known address of an adult person or the age and sex of any juvenile person cited, arrested, incarcerated or otherwise substantially deprived of liberty;

(k) whether the agency employed an automated license plate reader, wiretaps or other eavesdropping techniques, unless the release of this specific data would jeopardize an ongoing investigation;

(l) the manner in which the agencies received the information that led to the arrest and the names of individuals who supplied the information unless the identities of those individuals qualify for protection under subdivision 17; and

(m) response or incident report number.

Subd. 3. **Request for service data.** The following data created or collected by law enforcement agencies which document requests by the public for law enforcement services shall be public government data:

(a) the nature of the request or the activity complained of;

(b) the name and address of the individual making the request unless the identity of the individual qualifies for protection under subdivision 17;

(c) the time and date of the request or complaint; and

(d) the response initiated and the response or incident report number.

Subd. 4. **Audio recording of 911 call.** The audio recording of a call placed to a 911 system for the purpose of requesting service from a law enforcement, fire, or medical agency is private data on individuals with respect to the individual making the call, except that a written transcript of the audio recording is public, unless it reveals the identity of an individual otherwise protected under subdivision 17. A transcript shall be prepared upon request. The person requesting the transcript shall pay the actual cost of transcribing the call, in addition to any other applicable costs provided under section 13.03, subdivision 3. The audio recording may be disseminated to law enforcement agencies for investigative purposes. The audio recording may be used for public safety and emergency medical services training purposes.

Subd. 5. **Domestic abuse data.** The written police report required by section 629.341, subdivision 4, of an alleged incident described in section 629.341, subdivision 1, and arrest data, request for service data, and response or incident data described in subdivision 2, 3, or 6 that arise out of this type of incident or out of an alleged violation of an order for protection must be released upon request at no cost to the victim of domestic abuse, the victim's attorney, or an organization designated by the Office of Justice Programs in the Department of Public Safety as providing services to victims of domestic abuse. The executive director or the commissioner of the appropriate state agency shall develop written criteria for this designation.

Subd. 6. **Response or incident data.** The following data created or collected by law enforcement agencies which document the agency's response to a request for service including, but not limited to, responses to traffic accidents, or which describe actions taken by the agency on its own initiative shall be public government data:

(a) date, time and place of the action;

(b) agencies, units of agencies and individual agency personnel participating in the action unless the identities of agency personnel qualify for protection under subdivision 17;

(c) any resistance encountered by the agency;

(d) any pursuit engaged in by the agency;

(e) whether any weapons were used by the agency or other individuals;

(f) a brief factual reconstruction of events associated with the action;

(g) names and addresses of witnesses to the agency action or the incident unless the identity of any witness qualifies for protection under subdivision 17;

(h) names and addresses of any victims or casualties unless the identities of those individuals qualify for protection under subdivision 17;

(i) the name and location of the health care facility to which victims or casualties were taken;

(j) response or incident report number;

(k) dates of birth of the parties involved in a traffic accident;

(l) whether the parties involved were wearing seat belts; and

(m) the alcohol concentration of each driver.

Subd. 7. **Criminal investigative data.** Except for the data defined in subdivisions 2, 3, and 6, investigative data collected or created by a law enforcement agency in order to prepare a case against a person,

whether known or unknown, for the commission of a crime or other offense for which the agency has primary investigative responsibility are confidential or protected nonpublic while the investigation is active. Inactive investigative data are public unless the release of the data would jeopardize another ongoing investigation or would reveal the identity of individuals protected under subdivision 17. Photographs which are part of inactive investigative files and which are clearly offensive to common sensibilities are classified as private or nonpublic data, provided that the existence of the photographs shall be disclosed to any person requesting access to the inactive investigative file. An investigation becomes inactive upon the occurrence of any of the following events:

(a) a decision by the agency or appropriate prosecutorial authority not to pursue the case;

(b) expiration of the time to bring a charge or file a complaint under the applicable statute of limitations, or 30 years after the commission of the offense, whichever comes earliest; or

(c) exhaustion of or expiration of all rights of appeal by a person convicted on the basis of the investigative data.

Any investigative data presented as evidence in court shall be public. Data determined to be inactive under clause (a) may become active if the agency or appropriate prosecutorial authority decides to renew the investigation.

During the time when an investigation is active, any person may bring an action in the district court located in the county where the data are being maintained to authorize disclosure of investigative data. The court may order that all or part of the data relating to a particular investigation be released to the public or to the person bringing the action. In making the determination as to whether investigative data shall be disclosed, the court shall consider whether the benefit to the person bringing the action or to the public outweighs any harm to the public, to the agency or to any person identified in the data. The data in dispute shall be examined by the court in camera.

Subd. 8. **Child abuse identity data.** Active or inactive investigative data that identify a victim of child abuse or neglect reported under section 626.556 are private data on individuals. Active or inactive investigative data that identify a reporter of child abuse or neglect under section 626.556 are confidential data on individuals, unless the subject of the report compels disclosure under section 626.556, subdivision 11.

Subd. 9. **Inactive child abuse data.** Investigative data that become inactive under subdivision 7, clause (a) or (b), and that relate to the alleged abuse or neglect of a child by a person responsible for the child's care, as defined in section 626.556, subdivision 2, are private data.

Subd. 10. **Vulnerable adult identity data.** Active or inactive investigative data that identify a victim of vulnerable adult maltreatment under section 626.557 are private data on individuals. Active or inactive investigative data that identify a reporter of vulnerable adult maltreatment under section 626.557 are private data on individuals.

Subd. 11. **Inactive vulnerable adult maltreatment data.** Investigative data that becomes inactive under subdivision 7, paragraph (a) or (b), and that relate to the alleged maltreatment of a vulnerable adult by a caregiver or facility are private data on individuals.

Subd. 12. **Name change data.** Data on court records relating to name changes under section 259.10, subdivision 2, which is held by a law enforcement agency is confidential data on an individual while an investigation is active and is private data on an individual when the investigation becomes inactive.

Subd. 13. **Access to data for crime victims.** On receipt of a written request, the prosecuting authority shall release investigative data collected by a law enforcement agency to the victim of a criminal act or alleged criminal act or to the victim's legal representative unless the release to the individual subject of the data would be prohibited under section 13.821 or the prosecuting authority reasonably believes:

(a) that the release of that data will interfere with the investigation; or

(b) that the request is prompted by a desire on the part of the requester to engage in unlawful activities.

Subd. 14. **Withholding public data.** A law enforcement agency may temporarily withhold response or incident data from public access if the agency reasonably believes that public access would be likely to endanger the physical safety of an individual or cause a perpetrator to flee, evade detection or destroy evidence. In such instances, the agency shall, upon the request of any person, provide a statement which explains the necessity for its action. Any person may apply to a district court for an order requiring the agency to release the data being withheld. If the court determines that the agency's action is not reasonable, it shall order the release of the data and may award costs and attorney's fees to the person who sought the order. The data in dispute shall be examined by the court in camera.

Subd. 15. **Public benefit data.** Any law enforcement agency may make any data classified as confidential or protected nonpublic pursuant to subdivision 7 accessible to any person, agency, or the public if the agency determines that the access will aid the law enforcement process, promote public safety, or dispel widespread rumor or unrest.

Subd. 16. **Public access.** When data is classified as public under this section, a law enforcement agency shall not be required to make the actual physical data available to the public if it is not administratively feasible to segregate the public data from the not public. However, the agency must make the information described as public data available to the public in a reasonable manner. When investigative data becomes inactive, as described in subdivision 7, the actual physical data associated with that investigation, including the public data, shall be available for public access.

Subd. 17. **Protection of identities.** A law enforcement agency or a law enforcement dispatching agency working under direction of a law enforcement agency shall withhold public access to data on individuals to protect the identity of individuals in the following circumstances:

(a) when access to the data would reveal the identity of an undercover law enforcement officer, as provided in section 13.43, subdivision 5;

(b) when access to the data would reveal the identity of a victim or alleged victim of criminal sexual conduct or sex trafficking under section 609.322, 609.341 to 609.3451, or 617.246, subdivision 2;

(c) when access to the data would reveal the identity of a paid or unpaid informant being used by the agency if the agency reasonably determines that revealing the identity of the informant would threaten the personal safety of the informant;

(d) when access to the data would reveal the identity of a victim of or witness to a crime if the victim or witness specifically requests not to be identified publicly, unless the agency reasonably determines that revealing the identity of the victim or witness would not threaten the personal safety or property of the individual;

(e) when access to the data would reveal the identity of a deceased person whose body was unlawfully removed from a cemetery in which it was interred;

(f) when access to the data would reveal the identity of a person who placed a call to a 911 system or the identity or telephone number of a service subscriber whose phone is used to place a call to the 911 system and: (1) the agency determines that revealing the identity may threaten the personal safety or property of any person; or (2) the object of the call is to receive help in a mental health emergency. For the purposes of this paragraph, a voice recording of a call placed to the 911 system is deemed to reveal the identity of the caller;

(g) when access to the data would reveal the identity of a juvenile witness and the agency reasonably determines that the subject matter of the investigation justifies protecting the identity of the witness; or

(h) when access to the data would reveal the identity of a mandated reporter under section 609.456, 626.556, or 626.557.

Data concerning individuals whose identities are protected by this subdivision are private data about those individuals. Law enforcement agencies shall establish procedures to acquire the data and make the decisions necessary to protect the identity of individuals described in clauses (c), (d), (f), and (g).

Subd. 18. **Data retention.** Nothing in this section shall require law enforcement agencies to create, collect or maintain data which is not required to be created, collected or maintained by any other applicable rule or statute.

Subd. 19. **Data in arrest warrant indices.** Data in arrest warrant indices are classified as confidential data until the defendant has been taken into custody, served with a warrant, or appears before the court, except when the law enforcement agency determines that the public purpose is served by making the information public.

Subd. 20. **Property data.** Data that uniquely describe stolen, lost, confiscated, or recovered property are classified as either private data on individuals or nonpublic data depending on the content of the not public data.

Subd. 21. **Reward program data.** To the extent that the release of program data would reveal the identity of an informant or adversely affect the integrity of the fund, financial records of a program that pays rewards to informants are protected nonpublic data in the case of data not on individuals or confidential data in the case of data on individuals.

Subd. 22. **Data on registered criminal offenders.** Data described in section 243.166 shall be classified as described in that section.

Subd. 23. **Data in missing children bulletins.** Data described in section 299C.54 shall be classified as described in that section.

Subd. 24. **Exchanges of information.** Nothing in this chapter prohibits the exchange of information by law enforcement agencies provided the exchanged information is pertinent and necessary to the requesting agency in initiating, furthering, or completing an investigation, except not public personnel data and data governed by section 13.045.

Subd. 25. **Deliberative processes.** Data that reflect deliberative processes or investigative techniques of law enforcement agencies are confidential data on individuals or protected nonpublic data; provided that information, reports, or memoranda that have been adopted as the final opinion or justification for a decision of a law enforcement agency are public data.

Subd. 26. **Booking photographs.** (a) For purposes of this subdivision, "booking photograph" means a photograph or electronically produced image taken by law enforcement for identification purposes in connection with the arrest of a person.

(b) Except as otherwise provided in this subdivision, a booking photograph is public data. A law enforcement agency may temporarily withhold access to a booking photograph if the agency determines that access will adversely affect an active investigation.

Subd. 27. **Pawnshop and scrap metal dealer data.** Data that would reveal the identity of persons who are customers of a licensed pawnbroker, secondhand goods dealer, or a scrap metal dealer are private data on individuals. Data describing the property in a regulated transaction with a licensed pawnbroker, secondhand goods dealer, or a scrap metal dealer are public.

Subd. 28. **Disclosure of predatory offender registrant status.** Law enforcement agency disclosure to health facilities of the registrant status of a registered predatory offender is governed by section 244.052.

Subd. 29. **Juvenile offender photographs.** Notwithstanding section 260B.171, chapter 609A, or other law to the contrary, photographs or electronically produced images of children adjudicated delinquent under chapter 260B shall not be expunged from law enforcement records or databases.

Subd. 30. **Inactive financial transaction investigative data.** Investigative data that become inactive under subdivision 7 that are a person's financial account number or transaction numbers are private or nonpublic data.

Subd. 31. **Use of surveillance technology.** Notwithstanding subdivision 25 and section 13.37, subdivision 2, the existence of all technology maintained by a law enforcement agency that may be used to electronically capture an audio, video, photographic, or other record of the activities of the general public, or of an individual or group of individuals, for purposes of conducting an investigation, responding to an incident or request for service, monitoring or maintaining public order and safety, or engaging in any other law enforcement function authorized by law is public data.

History: *1979 c 328 s 21; 1981 c 311 s 36,39; 1982 c 545 s 24; 1982 c 558 s 1; 1984 c 552 s 2; 1985 c 298 s 30-36; 1986 c 444; 1988 c 625 s 1; 1989 c 177 s 1; 1989 c 351 s 12,13; 1990 c 402 s 1; 1991 c 285 s 1,2; 1991 c 319 s 9,10; 1993 c 351 s 16-18; 1994 c 618 art 1 s 14,15; 1994 c 636 art 4 s 3; 1995 c 229 art 3 s 1-3; 1995 c 231 art 2 s 2; 1995 c 259 art 1 s 19-23; art 4 s 3; 1996 c 440 art 1 s 16,17; 1997 c 85 art 5 s 1; 1998 c 371 s 4; 1999 c 227 s 22; 2000 c 445 art 2 s 1; 2002 c 352 s 7; 2004 c 269 art 1 s 1; 2004 c 290 s 16; 2005 c 136 art 3 s 1; 2005 c 163 s 49,50; 2006 c 260 art 3 s 2; 2007 c 54 art 7 s 1; 2012 c 216 art 15 s 4; 2012 c 290 s 54-58; 2013 c 76 s 7; 2013 c 125 art 1 s 2; 2014 c 212 art 1 s 1; 2015 c 65 art 6 s 2; 2015 c 67 s 1,2*