Data Practices for Employees:
Learn How to Not "Ring the Bell"

Presented to:

MASBO Conference

May 12, 2017

Presented by:

James K. Martin
Booth Law Group LLC
10520 Wayzata Boulevard
Minnetonka, MN 55305
Phone: 763-253-4155, ext. 7
Cell: 612-581-8450
Fax: 763-253-4160
e-mail: jmartin@boothlawgroup.com

This presentation was prepared by Booth Law Group LLC. It is not intended, nor should it be used, as a substitute for specific legal advice or opinion since legal counsel may only be given in response to inquiries regarding particular factual situations.
THE MINNESOTA GOVERNMENT DATA PRACTICES ACT

Tips for Handling Personnel Data

I. Introduction

The Minnesota Government Data Practices Act (Minnesota Statutes Chapter 13) has been developed in an attempt to balance two major public policy concerns. One concern is the public’s right to have access to information about their government. The policy of the public’s right to access must be balanced against the individual’s right to privacy. This balancing of the competing public policy concerns is best illustrated in Section 13.43 of the Data Practices Act which governs personnel data.

II. Personnel Data


B. The basic assumption throughout Data Practices Act is that all data held by the government is public information unless the provisions of the Data Practices Act designate the data as non-public.

C. Section 13.43, which governs personnel data, is just the opposite. In the case of personnel data, all data on public employees is considered private/non-public information unless it is designated public information by Section 13.43.

D. Rule of Thumb - Data on an employee will generally be designated public information if it is the type of information the public needs in order to make professional judgments about its public servants.

III. Access to Personnel Data

A. Public Data is always accessible to the public.

B. Authorization by the Subject of the Data (see attached authorization).

C. Court Order (usually when the employee/subject of the data is involved in litigation/legal dispute with an outside third party, for example, marriage dissolution).
D. Be cautious in making decisions to disclose; consult legal counsel if necessary.
   1. In weighing possible consequences, penalties for unlawful disclosure are more severe than inadvertent failure to disclose.
   2. Key Rule: “You Cannot Unring the Bell”!!

IV. Practice Tips

A. If possible, a request for personnel data should be in writing.
   1. Putting request in writing creates a record of the request and helps reduce confusion regarding what data is being requested.
   2. If the request for data is from a person/entity who is not the subject of the data, public employer cannot ask the requestor to identify him/herself or the reasons for the request.

B. Data Practices Act Does Not Require an Immediate Response to a Request for Personnel Data
   1. If the request is from someone who is not the subject of the data, response must be provided within a reasonable time.
   2. If the request is from a subject of the data, response must be immediate but if not immediate, within ten (10) days.
   3. If request cannot be granted (for example data is non-public or does not exist), written response must be provided describing why request cannot be granted.
   4. If requested data contains both public and non-public data, non-public data must be redacted. (However, see Burks v. Metropolitan Council, 884 N.W. 2d 338 (Minn. 2016 discussed below).

C. Inspection, Copies and Copy Costs
   1. If person requests data for purpose of “inspection” access must be provided to public data and costs may not be charged.
   2. Copies of public data must be provided upon request. If a requestor wants copies (including data transmitted electronically), he or she may be required to pay the actual costs of searching for and retrieving government data, including the cost of employee time, and for making, certifying,
compiling, copying, and/or electronically transmitting the data. An individual may not be charged for costs related to separating public from not public data. Cost of copies of 100 or fewer pages is 25 cents per page.

D. If data that is being sought is private information, employer must require production of authorization of the subject of the data and/or court order before private date is will be disclosed.

V. Tenessen Warning

A. When Minnesota public entity is seeking data (for example, conducting employment investigation).
   1. Why data is being collected

   2. Whether individual must provide data and consequences of either providing data or not providing data

   3. Individuals or entities who may have access to the data

B. Failure to provide Tenessen Warning in employee investigation may result in information that is gathered being deemed inadmissible in an arbitration hearing or other proceeding.

VI. Recent Development

A. Previously, if non-public data could not be separated from public data, then data could not be disclosed (for example, security video footage).

B. Change in law – Burks v. Metropolitan Council
   1. Ruling in Burks, which related to personnel data under Minn. Stat. § 13.43, states that subject of data must be granted access to data even if non-public data cannot be redacted.

   2. Burks creates possible conflict with disclosure of educational data governed by FERPA. As a federal law, FERPA may pre-empt the Data Practices Act.
AUTHORIZATION FOR THE RELEASE OF INFORMATION

If you have a question or would like more explanation about anything on this form, before you sign, please talk to:

<Name of Custodian of Data
Address
Phone number
Email address>

I, <name of employee or parent (as applicable)> and <name of student (if applicable)> authorize <Name of School or School District> ("District") to release data about me to <Recipient of Data> as described on this form.

The specific data I want the District to release:

<Specify data to be released>

I understand that my records are protected under state and/or federal privacy regulations and cannot be disclosed without my written consent unless otherwise provided by law.

I understand that I have asked the District to release the data.

I understand that although the data classified as private at the District, the classification or treatment of the data when released will depend upon any laws or policy that apply to <Recipient of the Data>.

I also understand that I may cancel this consent at any time prior to the information being released and that, in any event, this consent form expires automatically 90 days after signing.

I understand that by signing this informed consent to provide data to <Recipient of the Data>, data concerning <list of data to be disclosed> <consequences of disclosure, for example, what the recipient of the data might do with the data>.

Minnesota Statutes Section 13.05 requires automatic expiration of this authorization one year from the date of authorization.

________________________________________         

Date

________________________________________         

Date
DATA PRACTICES ACTIVITY

Based upon your review of Minn. Stat. Section 13.43 review the following list and decide whether the item is public information on employees or private information on employees.

1. Salary
2. Type or Level of Health Insurance
3. Warning Letter
4. Investigation of Harassment
5. Performance Reviews
6. Names of College(s) Attended
7. Discharge
8. Applicant
2016 Minnesota Statutes

13.43 PERSONNEL DATA.

Subdivision 1. Definition. As used in this section, "personnel data" means government data on individuals maintained because the individual is or was an employee of or an applicant for employment by, performs services on a voluntary basis for, or acts as an independent contractor with a government entity.

Subd. 2. Public data. (a) Except for employees described in subdivision 5 and subject to the limitations described in subdivision 5a, the following personnel data on current and former employees, volunteers, and independent contractors of a government entity is public:

(1) name; employee identification number, which must not be the employee's Social Security number; actual gross salary; salary range; terms and conditions of employment relationship; contract fees; actual gross pension; the value and nature of employer paid fringe benefits; and the basis for and the amount of any added remuneration, including expense reimbursement, in addition to salary;

(2) job title and bargaining unit; job description; education and training background; and previous work experience;

(3) date of first and last employment;

(4) the existence and status of any complaints or charges against the employee, regardless of whether the complaint or charge resulted in a disciplinary action;

(5) the final disposition of any disciplinary action together with the specific reasons for the action and data documenting the basis of the action, excluding data that would identify confidential sources who are employees of the public body;

(6) the complete terms of any agreement settling any dispute arising out of an employment relationship, including a buyout agreement as defined in section 123B.143, subdivision 2, paragraph (a); except that the agreement must include specific reasons for the agreement if it involves the payment of more than $10,000 of public money;

(7) work location; a work telephone number; badge number; work-related continuing education; and honors and awards received; and

(8) payroll time sheets or other comparable data that are only used to account for employee's work time for payroll purposes, except to the extent that release of time sheet data would reveal the employee's reasons for the use of sick or other medical leave or other not public data.

(b) For purposes of this subdivision, a final disposition occurs when the government entity makes its final decision about the disciplinary action, regardless of the possibility of any later proceedings or court proceedings. Final disposition includes a resignation by an individual when the resignation occurs after the final decision of the government entity, or arbitrator. In the case of arbitration proceedings arising under collective bargaining agreements, a final disposition occurs at the conclusion of the arbitration proceedings, or upon the failure of the employee to elect arbitration within the time provided by the collective bargaining agreement. A disciplinary action does not become public data if an arbitrator sustains a grievance and reverses all aspects of any disciplinary action.

(c) The government entity may display a photograph of a current or former employee to a prospective witness as part of the government entity's investigation of any complaint or charge against the employee.

(d) A complainant has access to a statement provided by the complainant to a government entity in connection with a complaint or charge against an employee.

(e) Notwithstanding paragraph (a), clause (5), and subject to paragraph (f), upon completion of an investigation of a complaint or charge against a public official, or if a public official resigns or is terminated from employment while the complaint or charge is pending, all data relating to the complaint or charge are public, unless access to the data would jeopardize an active investigation or reveal confidential sources. For purposes of this paragraph, "public official" means:
(1) the head of a state agency and deputy and assistant state agency heads;

(2) members of boards or commissions required by law to be appointed by the governor or other elective officers;

(3) executive or administrative heads of departments, bureaus, divisions, or institutions within state government; and

(4) the following employees:

(i) the chief administrative officer, or the individual acting in an equivalent position, in all political subdivisions;

(ii) individuals required to be identified by a political subdivision pursuant to section 471.701;

(iii) in a city with a population of more than 7,500 or a county with a population of more than 5,000: managers; chiefs; heads or directors of departments, divisions, bureaus, or boards; and any equivalent position; and

(iv) in a school district: business managers; human resource directors; athletic directors whose duties include at least 50 percent of their time spent in administration, personnel, supervision, and evaluation; chief financial officers; directors; individuals defined as superintendents and principals under Minnesota Rules, part 3512.0100; and in a charter school, individuals employed in comparable positions.

(f) Data relating to a complaint or charge against an employee identified under paragraph (e), clause (4), are public only if:

(1) the complaint or charge results in disciplinary action or the employee resigns or is terminated from employment while the complaint or charge is pending; or

(2) potential legal claims arising out of the conduct that is the subject of the complaint or charge are released as part of a settlement agreement.

This paragraph and paragraph (e) do not authorize the release of data that are made not public under other law.

Subd. 2a. Data disclosure by statewide pension plans. Notwithstanding any law to the contrary, with respect to data collected and maintained on members, survivors, and beneficiaries by statewide retirement systems that is classified as public data in accordance with subdivision 2, those retirement systems may be only required to disclose name, gross pension, and type of benefit awarded, except as required by sections 13.03, subdivisions 4 and 6; and 13.05, subdivisions 4 and 9.

Subd. 3. Applicant data. Except for applicants described in subdivision 5, the following personnel data on current and former applicants for employment by a government entity are public: veteran status; relevant test scores; rank on eligible list; job history; education and training; and work availability. Names of applicants shall be private data except when certified as eligible for appointment to a vacancy or when applicants are considered by the appointing authority to be finalists for a position in public employment. For purposes of this subdivision, "finalist" means an individual who is selected to be interviewed by the appointing authority prior to selection.

Subd. 4. Other data. All other personnel data is private data on individuals but may be released pursuant to a court order. Data pertaining to an employee’s dependents are private data on individuals.

Subd. 5. Undercover law enforcement officer. All personnel data maintained by a government entity relating to an individual employed as or an applicant for employment as an undercover law enforcement officer are private data on individuals. When the individual is no longer assigned to an undercover position, the data described in subdivisions 2 and 3 become public unless the law enforcement agency determines that revealing the data would threaten the personal safety of the officer or jeopardize an active investigation.

Subd. 5a. Limitation on disclosure of certain personnel data. Notwithstanding any other provision of this section, the following data relating to employees of a secure treatment facility defined in section 253B.02, subdivision 18a, employees of a state correctional facility, or employees of the Department of Corrections directly involved in supervision of offenders in the community, shall not be disclosed to facility patients,
corrections inmates, or other individuals who facility or correction administrators
reasonably believe will use the information to harass, intimidate, or assault any of these
employees: place where previous education or training occurred; place of prior
employment; and payroll timesheets or other comparable data, to the extent that disclosure
of payroll timesheets or other comparable data may disclose future work assignments,
home address or telephone number, the location of an employee during nonwork hours, or
the location of an employee's immediate family members.

Subd. 6. Access by labor organizations. Personnel data may be disseminated to
labor organizations to the extent that the responsible authority determines that the
dissemination is necessary to conduct elections, notify employees of fair share fee
assessments, and implement the provisions of chapters 179 and 179A. Personnel data shall
be disseminated to labor organizations and to the Bureau of Mediation Services to the
extent the dissemination is ordered or authorized by the commissioner of the Bureau of
Mediation Services.

Subd. 7. Employee assistance data. All data created, collected or maintained by a
government entity to administer employee assistance programs similar to the one
authorized by section 43A.319 are classified as private, pursuant to section 13.02,
subdivision 12. This section shall not be interpreted to authorize the establishment of
employee assistance programs.

Subd. 7a. Employee suggestion data. Personnel data includes data submitted by an
employee to a government entity as part of an organized self-evaluation effort by the
government entity to request suggestions from all employees on ways to cut costs, make
government more efficient, or improve the operation of government. An employee who is
identified in a suggestion shall have access to all data in the suggestion except the identity
of the employee making the suggestion.

Subd. 8. Harassment data. When allegations of sexual or other types of harassment
are made against an employee, the employee does not have access to data that would
identify the complainant or other witnesses if the responsible authority determines that the
employee's access to that data would:

(1) threaten the personal safety of the complainant or a witness; or

(2) subject the complainant or witness to harassment.

If a disciplinary proceeding is initiated against the employee, data on the complainant
or witness shall be available to the employee as may be necessary for the employee to
prepare for the proceeding.

Subd. 9. Peer counseling debriefing data. (a) Data acquired by a peer group
member in a public safety peer counseling debriefing is private data on the person being
debriefed.

(b) For purposes of this subdivision, "public safety peer counseling debriefing" means
a group process oriented debriefing session held for peace officers, firefighters, medical
emergency persons, dispatchers, or other persons involved with public safety emergency
services, that is established by any government entity providing public safety emergency
services and is designed to help a person who has suffered an occupation-related traumatic
event begin the process of healing and effectively dealing with posttraumatic stress.

Subd. 10. Prohibition on agreements limiting disclosure or discussion of
personnel data. (a) A government entity may not enter into an agreement settling a
dispute arising out of the employment relationship with the purpose or effect of limiting
access to or disclosure of personnel data or limiting the discussion of information or
opinions related to personnel data. An agreement or portion of an agreement that violates
this paragraph is void and unenforceable.

(b) Paragraph (a) applies to the following, but only to the extent that the data or
information could otherwise be made accessible to the public:

(1) an agreement not to discuss, publicize, or comment on personnel data or
information;

(2) an agreement that limits the ability of the subject of personnel data to release or
consent to the release of data; or
(3) any other provision of an agreement that has the effect of limiting the disclosure or discussion of information that could otherwise be made accessible to the public, except a provision that limits the ability of an employee to release or discuss private data that identifies other employees.

(c) Paragraph (a) also applies to a court order that contains terms or conditions prohibited by paragraph (a).

Subd. 11. Protection of employee or others. (a) If the responsible authority or designee of a government entity reasonably determines that the release of personnel data is necessary to protect an employee from harm to self or to protect another person who may be harmed by the employee, data that are relevant to the concerns for safety may be released as provided in this subdivision.

(b) The data may be released:

(1) to the person who may be harmed and to an attorney representing the person when the data are relevant to obtaining a restraining order;

(2) to a prepetition screening team conducting an investigation of the employee under section 253B.07, subdivision 1; or

(3) to a court, law enforcement agency, or prosecuting authority.

(c) Section 13.03, subdivision 4, paragraph (c), applies to data released under this subdivision, except to the extent that the data have a more restrictive classification in the possession of the agency or authority that receives the data. If the person who may be harmed or the person's attorney receives data under this subdivision, the data may be used or released further only to the extent necessary to protect the person from harm.

Subd. 12. Sharing of law enforcement personnel background investigation data. A law enforcement agency shall share data from a background investigation done under section 626.87 with the Peace Officer Standards and Training Board or with a law enforcement agency doing an investigation of the subject of the data under section 626.87.

Subd. 13. Dissemination of data to Department of Employment and Economic Development. Private personnel data must be disclosed to the Department of Employment and Economic Development for the purpose of administration of the unemployment benefits program under chapter 268.

Subd. 14. Maltreatment data. (a) When a report of alleged maltreatment of a student in a school facility, as defined in section 626.556, subdivision 2, paragraph (c), is made to the commissioner of education under section 626.556, data that are relevant to a report of maltreatment and are collected by the school facility about the person alleged to have committed maltreatment must be provided to the commissioner of education upon request for purposes of an assessment or investigation of the maltreatment report. Data received by the commissioner of education pursuant to these assessments or investigations are classified under section 626.556.

(b) Personnel data may be released for purposes of providing information to a parent, legal guardian, or custodian of a child under section 626.556, subdivision 7.

Subd. 15. Dissemination of data to law enforcement. Private personnel data, or data on employees that are confidential data under section 13.39, may be disseminated to a law enforcement agency for the purpose of reporting a crime or alleged crime committed by an employee, or for the purpose of assisting law enforcement in the investigation of a crime committed or allegedly committed by an employee.

Subd. 16. School district or charter school disclosure of violence or inappropriate sexual contact. The superintendent of a school district or the superintendent's designee, or a person having administrative control of a charter school, must release to a requesting school district or charter school private personnel data on a current or former employee related to acts of violence toward or sexual contact with a student, if:

(1) an investigation conducted by or on behalf of the school district or law enforcement affirmed the allegations in writing prior to release and the investigation resulted in the resignation of the subject of the data; or

(2) the employee resigned while a complaint or charge involving the allegations was pending, the allegations involved acts of sexual contact with a student, and the employer
informed the employee in writing, before the employee resigned, that if the employee resigns while the complaint or charge is still pending, the employer must release private personnel data about the employee's alleged sexual contact with a student to a school district or charter school requesting the data after the employee applies for employment with that school district or charter school and the data remain classified as provided in chapter 13.

Data that are released under this subdivision must not include data on the student.

Subd. 17. Continuity of operations. Personal home contact information may be used to ensure that an employee can be reached in the event of an emergency or other disruption affecting continuity of operation of a government entity. An employee's personal home contact information may be shared with another government entity in the event of an emergency or other disruption to ensure continuity of operation of either government entity.

Subd. 18. Private personnel data. Private personnel data of state employees must be disclosed to the Department of Administration for the purpose of administration of the workers' compensation program as provided in chapter 176.

Subd. 19. Employee of contractor or subcontractor. The following data maintained as a result of a contractual relationship entered on or after August 1, 2012, between a government entity and a contractor or subcontractor are private: the personal telephone number, home address, and e-mail address of a current or former employee of the contractor or subcontractor. A government entity maintaining data under this subdivision must share the data with another government entity to perform a function authorized by law. The data must be disclosed to a government entity or any person for prevailing wage purposes.

History: 1979 c 328 s 17; 1980 c 603 s 24, 25, 29; 1981 c 311 s 12, 13, 17, 39; 1982 c 545 s 9, 10, 24; 1984 c 436 s 17; 1984 c 544 s 89; 1985 c 298 s 12; 1987 c 186 s 15; 1987 c 284 art I s 1; 1987 c 351 s 7; 1987 c 384 art I s 2; 1988 c 598 s 1; 1990 c 550 s 1; 1991 c 319 s 4-6; 1993 c 351 s 6, 7; 1994 c 618 art I s 9; 1995 c 259 art I s 7-9; 1995 c 3 art 9 s 1; 1996 c 440 art I s 10-12; 1997 c 214 s 2; 1998 c 397 art I s 3; 1999 c 107 s 66; 1999 c 182 s 1; 1999 c 227 s 6; 1999 c 250 art I s 114; 2000 c 343 s 4; 2001 c 70 s 1; 2001 c 178 art 2 s 3; 2002 c 243 s 1; 2002 c 352 s 6; 2002 c 396 s 1; 2003 c 130 s 12; 1Sp2003 c 8 art I s 8; 2004 c 137 s 1; 2004 c 206 s 52; 2004 c 288 art I s 1, 2; 2004 c 290 s 4; 2004 c 290 s 5; 2005 c 163 s 37-39; 2007 c 129 s 23-28; 2009 c 142 art I s 1, 2; 2010 c 365 art I s 3, 4; 2012 c 280 s 1; 2012 c 290 s 21-23; 2013 c 82 s 4, 5; 2014 c 312 art I s 1, 2; 2015 c 71 art I s 126

Copyright © 2016 by the Revisor of Statutes, State of Minnesota. All rights reserved.