

## **Legal Risk Analysis Tool: Consequences by Minnesota Government Data Practices Act Classification**

For information regarding the Minnesota Government Data Practices Act, please refer to Appendix D of the Trustworthy Information Systems Handbook.

For information specifically regarding legal issues affecting electronic records management, please refer to Appendix E of the Trustworthy Information Systems Handbook.

### **DATA ON INDIVIDUALS:**

- Public data on individuals**
- Private data on individuals**
- Confidential data on individuals**
- Public data on decedents**
- Private data on decedents**
- Confidential data on decedents**

### **DATA NOT ON INDIVIDUALS:**

- Public data**
- Non-public data**
- Protected, non-public data**

### **A1. POTENTIAL LEGAL RISKS IF DATA ON INDIVIDUALS ARE LOST OR STOLEN:**

1. Anyone who allows or carries out the unauthorized destruction, removal, mutilation, concealment, alteration, defacement, or obliteration of a government record is guilty of a misdemeanor under Minnesota Statutes, section 138.225.
2. Any person who willfully violates the provisions of the Minnesota Government Data Practices Act or any rules adopted under it is guilty of a misdemeanor. (See Minnesota Rules, chapter 1205 for the rule text.) Willful violation of the Act by any public employee constitutes just cause for suspension without pay or dismissal of the public employee under Minnesota Statutes, section 13.09.
3. If data are lost or stolen, you will be in violation of Minnesota Statute 13.05, subd. 5, which requires government data about individuals to be accurate, complete, and current and that there are appropriate security safeguards to protect them.
4. You may be subject to a lawsuit by the individual to whom the data pertains for negligence in maintaining the data in compliance with the statutory requirements. You may be forced to pay any damages sustained, plus costs and reasonable attorney fees; if a

willful violation is proved, you may be liable to pay exemplary damages under Minnesota Statutes, section 13.08, subd. 1. An individual who claims s/he was damaged because data are lost or stolen must show that the damage is the direct result of the loss or theft of the public data.

5. If the data are lost, the credibility of your other data may be challenged in a lawsuit, or the fact that data were lost may be used as evidence of negligence in your data management practices or evidence of ineffective data management procedures.
6. If the data are stolen, your security measures and access restrictions may be called into question, which may affect the credibility of your other data.
7. You may spend a lot of time and expense looking for data that are lost or stolen, and you may be required to give third parties access to your records and data systems to ensure that such data are indeed lost or stolen, and that you are not just refusing to turn the data over to them.
8. You may be subject to damages, fines and/or penalties if data that are lost or stolen are required to be maintained by law, if you are contractually committed to maintain such data, or if you must protect data from inappropriate disclosure.
9. If data are lost or stolen, you may suffer economic loss (e.g., being unable to sell the data yourself) arising from the loss of ownership and control of the data.
10. You may not be able to complete reporting requirements imposed by the state or federal government or other parties which could result in termination of a federal or state program or loss of funding.
11. You may not be able to provide evidence of compliance with state, local, and federal regulations.
12. You are unable to produce the data in a lawsuit in which you are a party. This may harm you if (a) the data contained information that would be useful in your defense; or (b) the data were requested by the other party and you cannot produce them. This can also lead to an inference against you that you destroyed the data because they were detrimental to you, especially if you have records retention schedules and did not follow them in connection with the data in question or if you have no records retention schedules to cover the data in question. In addition, evidence that you did not follow your records retention schedules can be used as evidence of recklessness or intentional obstruction of justice, especially if you were on notice that the data may be relevant to a person's claim before you destroyed them. You could also be subjected to contempt of court or a ruling against you.
13. You do not need to be a party to a lawsuit to be asked to provide data. If not public data are requested, you are required to protect any classified data while producing those data that are appropriate. There is a process in Minnesota Statutes, section 13.03, subd. 6 that

may be used to determine whether not public data are released. If you receive a data practices request, a discovery request, or a subpoena for not public data, the best thing to do is contact your lawyer for directions.

## **A2. POTENTIAL LEGAL RISKS IF DATA NOT ON INDIVIDUALS ARE LOST OR STOLEN:**

1. Anyone who allows or carries out the unauthorized destruction, removal, mutilation, concealment, alteration, defacement, or obliteration of a government record is guilty of a misdemeanor under Minnesota Statutes, section 138.225.
2. Any person who willfully violates the provisions of the Minnesota Government Data Practices Act is guilty of a misdemeanor. Willful violation of the Act by any public employee constitutes just cause for suspension without pay or dismissal of the public employee under Minnesota Statutes, section 13.09.
3. If data are lost or stolen, you will be in violation of Minnesota Statute 13.03, subd. 1, which requires government data to be in such a condition and arrangement as to make them easily accessible for convenient use.
4. If your data are lost or stolen, you may suffer economic loss (e.g., being unable to sell the data yourself) arising from the loss of ownership and therefore loss of control of the data.
5. You may be liable (e.g., fines, penalties, damages) for breach of contract if the terms of a contract include requirements such as records retention or non-disclosure.
6. You may not be able to complete reporting requirements imposed by the state or federal government or other parties which could result in termination of a federal or state program or loss of funding.
7. You may not be able to provide evidence of compliance with state, local, and federal regulations.
8. You may be subject to negligence or personal injury lawsuits if the loss of information results in damage or injury to any third party.
9. If the data are lost, the credibility of your other data may be challenged in a lawsuit, or the fact that data were lost may be used as evidence of negligence in your data management practices or evidence of ineffective data management procedures.
10. If the data are stolen, your security measures and access restrictions may be called in into question, which may impact the credibility of your other data.
11. You may spend a lot of time and expense looking for data that are lost or stolen, and you may be required to give third parties access to your records and data systems to ensure

that such data are indeed lost or stolen, and that you are not just refusing to turn the data over to them.

12. You may be subject to a lawsuit for negligence in maintaining the data in compliance with the statutory requirements.
13. You are unable to produce the data in a lawsuit to which you are a party. This may harm you if (a) the data contained information that would be useful in your defense; or (b) the data were requested by the other party and you cannot produce them. This can also lead to an inference against you that you destroyed the data because they were detrimental to you, especially if you have records retention schedules and did not follow them in connection with the data in question or if you have no records retention schedules to cover the data in question. In addition, evidence that you did not follow your records retention schedules can be used as evidence of recklessness or intentional obstruction of justice, especially if you were on notice that the data may be relevant to a person's claim before you destroyed them. You could also be subjected to contempt of court or a ruling against you.
14. You do not need to be a party to a lawsuit to be asked to provide data. If not public data are requested, you are required to protect any classified data while producing those data that are appropriate. There is a process in Minnesota Statutes, section 13.03, subd. 6 that may be used to determine whether not public data are released. If you receive a data practices request, a discovery request or a subpoena for not public data, the best thing to do is contact your lawyer for directions.

## **B1. POTENTIAL LEGAL RISKS IF DATA ON INDIVIDUALS ARE INAPPROPRIATELY DESTROYED:**

1. Anyone who allows or carries out the unauthorized destruction, removal, mutilation, concealment, alteration, defacement, or obliteration of a government record is guilty of a misdemeanor under Minnesota Statutes, section 138.225.
2. Any person who willfully violates the provisions of the Minnesota Government Data Practices Act or any rules adopted under it is guilty of a misdemeanor. (See Minnesota Rules, chapter 1205 for rule text.) Willful violation of the Act by any public employee constitutes just cause for suspension without pay or dismissal of the public employee under Minnesota Statutes, section 13.09.
3. If data are inappropriately destroyed, you will be in violation of Minnesota Statutes, section 13.05, subd. 5, which requires government data about individuals to be accurate, complete and current and that there are appropriate security safeguards to protect them.
4. You may be subject to a lawsuit by the individual to whom the data pertains for negligence in maintaining the data in compliance with the statutory requirements. You may be forced to pay any damages sustained, plus costs and reasonable attorney fees; if a

willful violation is proved, you may be liable to exemplary damages under Minnesota Statutes, section 13.08, subd. 1. An individual who claims that s/he was damaged because data are inappropriately destroyed must show the damage is the direct result of the inappropriate destruction.

5. If your data are stolen or lost, you may suffer economic loss (e.g., being unable to sell the data yourself) arising from the loss of ownership and loss of control of the data.
6. You may spend a lot of time and expense looking for data that are destroyed, and you may be required to give third parties access to your records and data systems to ensure that such data are indeed lost or stolen, and that you are not just refusing to turn the data over to them.
7. You may be subject to damages, fines and/or penalties if data that are destroyed are required to be maintained by law or if you are contractually committed to maintain such data.
8. You may not be able to complete reporting requirements imposed by the state or federal government or other parties which could result in termination of a federal or state program or loss of funding.
9. You may not be able to provide evidence of compliance with state, local, and federal regulations.
10. You are unable to produce the data in a lawsuit in which you are a party. This may harm you if (a) the data contained information that would be useful in your defense; or (b) the data were requested by the other party and you cannot produce them. This can also lead to an inference against you that you destroyed the data because they were detrimental to you, especially if you have records retention schedules and did not follow them in connection with the data in question or if you have no records retention schedules to cover the data in question. In addition, evidence that you did not follow your records retention schedules can be used as evidence of recklessness or intentional obstruction of justice, especially if you were on notice that the data may be relevant to a person's claim before you destroyed them. You could also be subjected to contempt of court or a ruling against you.
11. You do not need to be a party to a lawsuit to be asked to provide data. If not public data are requested, you are required to protect any classified data while producing those data that are appropriate. There is a process in Minnesota Statutes, section 13.03, subd. 6 that may be used to determine whether not public data are released. If you receive a data practices request, a discovery request or a subpoena for not public data, the best thing to do is contact your lawyer for directions.

## **B2. POTENTIAL LEGAL RISKS IF DATA NOT ON INDIVIDUALS ARE INAPPROPRIATELY DESTROYED:**

1. Anyone who allows or carries out the unauthorized destruction, removal, mutilation, concealment, alteration, defacement, or obliteration of a government record is guilty of a misdemeanor under Minnesota Statutes, section 138.225.
2. Any person who willfully violates the provisions of the Minnesota Government Data Practices Act is guilty of a misdemeanor. Willful violation of the Act by any public employee constitutes just cause for suspension without pay or dismissal of the public employee under Minnesota Statutes, section 13.09.
3. If data are inappropriately destroyed, you will be in violation of Minnesota Statute 13.03, subd. 1, which requires government data to be in such a condition and arrangement as to make them easily accessible for convenient use.
4. You may be liable (e.g., fines, penalties, damages) for breach of contract if the terms of a contract include requirements such as records retention or confidentiality.
5. You may not be able to complete reporting requirements imposed by the state or federal government or other parties (which could result in termination of a federal or state program or loss of funding).
6. You may not be able to provide evidence of compliance with state, local, and federal regulations.
7. You may be subject to negligence or personal injury lawsuits if the loss of information results in damage or injury to any third party.
8. You may spend a lot of time and expense looking for data that are destroyed (if you don't have a record of its being destroyed in connection with your records retention schedules), and you may be required to give third parties access to your records and data systems to ensure that such data are indeed destroyed, and that you are not just refusing to turn the data over to them.
9. You may be subject to a lawsuit for negligence in maintaining the data in compliance with the statutory requirements.
10. You are unable to produce the data in a lawsuit to which you are a party. This may harm you if (a) the data contained information that would be useful in your defense; or (b) the data were requested by the other party and you cannot produce them. This can also lead to an inference against you that you destroyed the data because they were detrimental to you, especially if you have records retention schedules and did not follow them in connection with the data in question or if you have no records retention schedules to cover the data in question. In addition, evidence that you did not follow your records retention schedules can be used as evidence of recklessness or intentional obstruction of

justice, especially if you were on notice that the data may be relevant to a person's claim before you destroyed them. You could also be subjected to contempt of court or a ruling against you.

11. You do not need to be a party to a lawsuit to be asked to provide data. If not public data are requested, you are required to protect any classified data while producing those data that are appropriate. There is a process in Minnesota Statutes, section 13.03, subdivision 6 that may be used to determine whether not public data are released. If you receive a data practices request, a discovery request or a subpoena for not public data, the best thing to do is contact your lawyer for directions.

## **C1. POTENTIAL LEGAL RISKS IF DATA ON INDIVIDUALS ARE INACCURATE OR CORRUPTED:**

1. Anyone who allows or carries out the unauthorized destruction, removal, mutilation, concealment, alteration, defacement, or obliteration of a government record is guilty of a misdemeanor under Minnesota Statutes, section 138.225.
2. Any person who willfully violates the provisions of the Minnesota Government Data Practices Act or any rules adopted under it is guilty of a misdemeanor. (See Minnesota Rules, chapter 1205 for rule text.) Willful violation of the Act by any public employee constitutes just cause for suspension without pay or dismissal of the public employee under Minnesota Statutes, section 13.09.
3. An individual data subject may challenge the accuracy and completeness of public and private data about them under Minnesota Statutes, section 13.04, subd. 4.
4. You may be subject to a lawsuit by the individual to whom the data pertains for negligence in maintaining the data in compliance with the statutory requirements. You may be forced to pay any damages sustained, plus costs and reasonable attorney fees; if a willful violation is proved, you may be liable to exemplary damages under Minnesota Statutes, section 13.08, subd. 1. An individual who claims s/he was damaged because data are inaccurate or corrupted must show the damage is the direct result of the inaccuracy or corruption.
5. Your procedures and internal controls (such as security measures and access restriction) are discredited, which may be used against you in determining the credibility of other data, whether it be (a) in court to be used as evidence; or (b) in connection with reporting to federal or state agencies, or private accrediting bodies. In addition, your credibility is compromised, which may harm or destroy relationships with third parties. You may also have violated Minnesota Statutes, section 13.05, subd. 5 which requires that data about individuals be protected with appropriate security safeguards.
6. Inaccurate or corrupted data may be used as evidence of negligence or recklessness with respect to data management.

7. You may be subject to damages, fines and/or penalties if data you are required by law or contractual obligation to maintain becomes inaccurate or corrupted.
8. Inaccurate or corrupted data may not be admitted into evidence in court; therefore, such data may not be used in your defense in any lawsuit.
9. You may not be able to complete reporting requirements imposed by the state or federal government or other parties which could result in termination of a federal or state program or loss of funding.
10. You may not be able to provide evidence of compliance with state, local, and federal regulations.

## **C2. POTENTIAL LEGAL RISKS IF DATA NOT ON INDIVIDUALS ARE INACCURATE OR CORRUPTED:**

1. Anyone who allows or carries out the unauthorized destruction, removal, mutilation, concealment, alteration, defacement, or obliteration of a government record is guilty of a misdemeanor under Minnesota Statutes, section 138.225.
2. Any person who willfully violates the provisions of the Minnesota Government Data Practices Act is guilty of a misdemeanor. Willful violation of the Act by any public employee constitutes just cause for suspension without pay or dismissal of the public employee under Minnesota Statutes, section 13.09.
3. You may be liable (e.g., fines, penalties, damages) for breach of contract if the terms of a contract include requirements such as records retention.
4. You may not be able to complete reporting requirements imposed by the state or federal government or other parties (which could result in termination of a federal or state program or loss of funding).
5. You may not be able to provide evidence of compliance with state, local, and federal regulations.
6. You may be subject to negligence or personal injury lawsuits if the loss of information results in damage or injury to any third party.
7. Your procedures and internal controls (such as security measures and access restriction) are discredited, which may be used against you in determining the credibility of other data, whether it be (a) in court to be used as evidence; or (b) in connection with reporting to the federal government or other federal or state agencies or private accrediting bodies. In addition, your credibility is compromised, which may harm or destroy relationships with third parties.

8. Inaccurate or corrupted data may be used as evidence of negligence or recklessness with respect to data management.
9. Inaccurate or corrupted data may not be admitted into evidence in court; therefore no such data may be used in your defense in any lawsuit.
10. You may be liable for defamation to a corporation or other corporate entity if the information is disseminated to a third party.
11. You may be liable for negligence if the data were relied upon by a third party to its detriment.

#### **D1. POTENTIAL LEGAL RISKS IF DATA ON INDIVIDUALS ARE MISUSED:**

1. Any person who willfully violates the provisions of the Minnesota Government Data Practices Act or any rules adopted under it is guilty of a misdemeanor. (See Minnesota Rules, chapter 1205 for rule text.) Willful violation of the Act by any public employee constitutes just cause for suspension without pay or dismissal of the public employee under Minnesota Statutes, section 13.09.
2. You may be subject to a lawsuit by the individual to whom the data pertains for negligence in maintaining the data in compliance with the statutory requirements. You may be forced to pay any damages sustained, plus costs and reasonable attorney fees; if a willful violation is proved, you may be liable to exemplary damages under Minnesota Statutes, section 13.08, subd. 1. An individual who claims s/he was damaged because data are misused must show the damage is the direct result of the misuse.
3. Your procedures and internal controls (such as security measures and access restriction) are discredited, which may be used against you in determining the credibility of other data, whether it be (a) in court to be used as evidence; or (b) in connection with reporting to federal or state agencies, or private accrediting bodies. In addition, your credibility is compromised, which may harm or destroy relationships with third parties. You may have violated Minnesota Statutes, section 13.05, subd. 5 which requires that data about individuals be protected with appropriate security safeguards.
4. The misuse of data may be used as evidence of negligence or recklessness with respect to data management.
5. You may be subject to damages, fines and/or penalties if data that are required to be maintained by law or that you are contractually committed to maintain are misused.

## **D2. POTENTIAL LEGAL RISKS IF DATA NOT ON INDIVIDUALS ARE MISUSED:**

1. Misuse of data not on individuals occurs only if non-public or protected non-public data are disclosed inappropriately.
2. Any person who willfully violates the provisions of the Minnesota Government Data Practices Act or any rules adopted under it is guilty of a misdemeanor. Willful violation of the Act by any public employee constitutes just cause for suspension without pay or dismissal of the public employee under Minnesota Statutes, section 13.09.
3. You may be liable (e.g., fines, penalties, damages) for breach of contract if the terms of a contract include requirements such as records retention or non-disclosure.
4. You may be subject to negligence lawsuits if the loss of information results in damage or injury to any third party.
5. Your procedures and internal controls (such as security measures and access restriction) are discredited, which may be used against you in determining the credibility of other data, whether it be (a) in court to be used as evidence; or (b) in connection with reporting to federal or state agencies, or private accrediting bodies. In addition, your credibility may be compromised, which may harm or destroy relationships with third parties.

## **E1. POTENTIAL LEGAL RISKS IF DATA ON INDIVIDUALS ARE MISHANDLED OR NOT SECURE/RESTRICTED ACCESS:**

1. Any person who willfully violates the provisions of the Minnesota Government Data Practices Act or any rules adopted under it is guilty of a misdemeanor. (See Minnesota Rules, chapter 1205 for rule text.) Willful violation of the Act by any public employee constitutes just cause for suspension without pay or dismissal of the public employee under Minnesota Statutes, section 13.09.
2. You may be subject to a lawsuit by the individual to whom the data pertains for negligence in maintaining the data in compliance with the statutory requirements. You may be forced to pay any damages sustained, plus costs and reasonable attorney fees; if a willful violation is proved, you may be liable to exemplary damages under Minnesota Statutes, section 13.08, subd. 1. An individual who claims s/he was damaged because data are mishandled/not secure/or accessed inappropriately must show the damage is the direct result of the mishandling, lack of security or inappropriate access.
3. If you exchange private or confidential data with other government entities without the informed consent of the data subject(s) or without statutory authority, you may be in violation of Minnesota Statutes, section 13.05, subd. 4b.
4. Your procedures and internal controls (such as security measures and access restriction) are discredited, which may be used against you in determining the credibility of other

data, whether it be (a) in court to be used as evidence; or (b) in connection with reporting federal or state agencies, or private accrediting bodies. In addition, your credibility is compromised, which may harm or destroy relationships with third parties. You may also have violated Minnesota Statutes, section 13.05, subd. 5 which requires that data about individuals be protected with appropriate security safeguards.

5. Mishandled or unsecured data may be used as evidence of negligence or recklessness with respect to data management.
6. You may be subject to damages, fines and/or penalties if data you are required by law or contract to maintain are mishandled or not secured.
7. Data may not be admitted into evidence in court if they are unsecured and trustworthiness cannot be proven; therefore, such data may not be used in your defense in any lawsuit.
8. You may not be able to complete reporting requirements imposed by the state or federal government or other parties (which could result in termination of a federal or state program or loss of funding).

## **E2. POTENTIAL LEGAL RISKS IF DATA NOT ON INDIVIDUALS ARE MISHANDLED OR NOT SECURE/RESTRICTED ACCESS:**

1. Any person who willfully violates the provisions of the Minnesota Government Data Practices Act is guilty of a misdemeanor. Willful violation of the Act by any public employee constitutes just cause for suspension without pay or dismissal of the public employee under Minnesota Statutes, section 13.09.
2. You may be liable (e.g., fines, penalties, damages) for breach of contract if the terms of a contract include requirements such as records retention or confidentiality.
3. You may be subject to negligence or personal injury lawsuits if the loss of information results in damage or injury to any third party.
4. If your procedures and internal controls (such as security measures and access restriction) are discredited, this may be used against you in determining the credibility of other data, whether it be (a) in court to be used as evidence; or (b) in connection with reporting to federal or state agencies, or private accrediting bodies. In addition, if your credibility is compromised, this may harm or destroy relationships with third parties.
5. Mishandled or unsecured data may be used as evidence of negligence or recklessness with respect to data management.
6. Data may not be admitted into evidence in court if they are unsecured and trustworthiness cannot be proven; therefore, it is unlikely this type of data will be used in your defense in

any lawsuit.

## **F1. POTENTIAL LEGAL RISKS IF DATA ON INDIVIDUALS ARE REQUIRED AS EVIDENCE IN LITIGATION BUT ARE NOT AVAILABLE:**

1. You are unable to produce the data in a lawsuit in which you are a party. This may harm you if (a) the data contained information that would be useful in your defense; or (b) the data were requested by the other party and you cannot produce it. This can also lead to an inference against you that you destroyed the data because it was detrimental to you, especially if you have records retention schedules and did not follow them in connection with the data in question or if you have no records retention schedules to cover the data in question. In addition, evidence that you did not follow your records retention schedules can be used as evidence of recklessness or intentional obstruction of justice, especially if you were on notice that the data may be relevant to a person's claim before you destroyed it. You could also be subjected to contempt of court or a ruling against you.
2. You do not need to be a party to a lawsuit to be asked to provide data. If not public data are requested, you are required to protect any classified data while producing those data that are appropriate. There is a process in Minnesota Statutes, section 13.03, subd. 6 that may be used to determine whether not public data are released. If you receive a data practices request, a discovery request or a subpoena for not public data, the best thing to do is contact your lawyer for directions.
3. If data are required for litigation but are not available, you may be in violation of Minnesota Statutes, section 13.05, subd. 5, which requires government data about individuals to be accurate, complete and current and that there are appropriate security safeguards to protect the data.
4. The credibility of your other data may be challenged in a lawsuit, or the fact that data are not available may be used as evidence of negligence in your data management practices or evidence of ineffective data management procedures.
5. Your security measures and access restrictions may be called into question, which may impact the credibility of your other data.
6. You may spend a lot of time and expense looking for data that are not available, and you may be required to give third parties access to your records and data systems to ensure that such data are indeed unavailable, and that you are not just refusing to turn the data over to them.

**F2. POTENTIAL LEGAL RISKS IF DATA NOT ON INDIVIDUALS ARE REQUIRED AS EVIDENCE IN LITIGATION BUT ARE NOT AVAILABLE:**

1. If data are required for litigation but are not available, you will be in violation of Minnesota Statutes, section 13.03, subd. 1, which requires government data to be in such a condition and arrangement as to make them easily accessible for convenient use.
2. You may be liable (e.g., fines, penalties, damages) for breach of contract if the terms of a contract include requirements such as records retention.
3. You may not be able to provide evidence of compliance with state, local, and federal regulations.
4. If the data are lost, the credibility of your other data may be challenged in a lawsuit, or the fact that data were lost may be used as evidence of negligence in your data management practices or evidence of ineffective data management procedures.
5. If the data are stolen, your security measures and access restrictions may be called in into question, which may impact the credibility of your other data.
6. You may spend a lot of time and expense looking for data that are lost or stolen, and you may be required to give third parties access to your records and data systems to ensure that such data are indeed lost or stolen, and that you are not just refusing to turn the data over to them.
7. Inaccurate or corrupted data may be used as evidence of negligence or recklessness with respect to data management.
8. You are unable to produce the data in a lawsuit to which you are a party. This may harm you if (a) the data contained information that would be useful in your defense; or (b) the data were requested by the other party and you cannot produce them. This can also lead to an inference against you that you destroyed the data because they were detrimental to you, especially if you have records retention schedules and did not follow them in connection with the data in question or if you have no records retention schedules to cover the data in question. In addition, evidence that you did not follow your records retention schedules can be used as evidence of recklessness or intentional obstruction of justice, especially if you were on notice that the data may be relevant to a person's claim before you destroyed them. You could also be subjected to contempt of court or a ruling against you.
9. You do not need to be a party to a lawsuit to be asked to provide data. If not public data are requested, you are required to protect any classified data while producing those data that are appropriate. There is a process in Minnesota Statutes, section 13.03, subdivision 6 that may be used to determine whether not public data are released. If you receive a data practices request, a discovery request or a subpoena for not public data, the best thing to do is contact your lawyer for directions.

**G1. POTENTIAL LEGAL RISKS IF DATA ON INDIVIDUALS ARE REQUIRED FOR AUDIT PURPOSES BUT ARE NOT AVAILABLE:**

1. If data are required for audit purposes but are not available, you will be in violation of Minnesota Statutes, section 13.05, subd. 5, which requires government data about individuals to be accurate, complete and current and that there are appropriate security safeguards to protect the data.
2. You may be liable (e.g., fines, penalties, damages) for breach of contract if the terms of a contract include requirements such as records retention, and gives the other party to the contract the right to audit your records to ensure compliance with such requirements.

**G2. POTENTIAL LEGAL RISKS IF DATA NOT ON INDIVIDUALS ARE REQUIRED FOR AUDIT PURPOSES BUT ARE NOT AVAILABLE:**

1. If data are required for audit but are not available, you will be in violation of Minnesota Statutes, section 13.03, subd. 1, which requires government data to be in such a condition and arrangement as to make them easily accessible for convenient use.
2. You may be liable (e.g., fines, penalties, damages) for breach of contract if the terms of a contract include requirements such as records retention and gives the other party to the contract the right to audit your records to ensure compliance with such requirements.