State of Wisconsin
2023 - 2024 LEGISLATURE

LRB-2528/1
MDE:amn

2023 ASSEMBLY BILL 824

December 22, 2023 - Introduced by Representatives ZIMMERMAN, GUSTAFSON, MICHALSKI, BINSFELD and MAXEY. Referred to Committee on State Affairs.

AUTHORS SUBJECT TO CHANGE

AN ACT ***to create*** 100.75 of the statutes; **relating to:** establishing standards for the sharing of sensitive information between separate legal entities.

Analysis by the Legislative Reference Bureau

This bill establishes requirements, standards, and collaborative requirements for entities that own, control, and share personal data. The bill governs three types of data controllers: 1) data owners, meaning any person that generates, collects, or uses data for its own purposes; 2) data custodians, meaning any person that provides data security and storage on behalf of a data owner; and 3) data stewards, meaning any person that uses or facilitates the use of data on behalf of a data owner.

Data is defined in the bill as including "sensitive information," which is defined as information that, if disclosed or accessed by unauthorized parties, could result in harm, privacy violations, or negative consequences for individuals or entities. "Sensitive information" includes "personally identifiable information," meaning information that is or can reasonably be linked to an identified person, identifiable person, or device linked to a person, and "nonpublic or privately held information," meaning information that is not publicly available or accessible to the general public; is restricted to a specific group of individuals or entities; is considered confidential or proprietary; is protected by privacy regulations; and requires appropriate safeguards to prevent unauthorized access, use, or disclosure. The requirements of the bill apply to data controllers who use or facilitate the use of sensitive information.

Under the bill, a data owner must limit the access to, sharing of, and use of its data to what is adequate, relevant, and reasonably necessary for the purposes for which the data is collected or generated. A data owner must also establish and

ensure compliance with relevant regulatory requirements and with internal policies related to the review of data sharing and data use requests; data handling best practices; and the handling of data agreement breaches, security incidents, and related disputes.

Under the bill, a data custodian must provide a secure environment for the storage of a data owner's data that is designed and configured in a manner that reflects best practices in data security on subjects including identity and access management controls, role–based permissions, data encryption, cyber security threat monitoring, and recovery capabilities in the event of a disaster. A data custodian must also establish and ensure compliance with internal policies and procedures related to data access control, data retention and data destruction, auditing capabilities and the performance of audits, the periodic review of new and changing business and regulatory requirements that may impact data solution organization, and any other requirements established in a data agreement. A data custodian must also establish and ensure compliance with internal policies and procedures related to security incidents and auditing.

Under the bill, a data steward must establish and ensure compliance with internal policies and procedures related to various data handling practices.

If a data owner enters into an agreement with a data custodian or a data steward, the agreement must meet the requirements described in the bill. Such an agreement must identify all relevant parties, data sets, permitted uses and restrictions of data, confidentiality requirements, law governing the data, and law governing the agreement. Such an agreement must also include statements regarding the response to security incidents, the term of the agreement, the terms for terminating the agreement, and the authorization for or prohibition of the collection and analysis of metadata, or data that describes other data. Such an agreement between a data owner and a data custodian must include statements regarding auditing capabilities and requirements.

The people of the state of Wisconsin, represented in senate and assembly, do enact as follows:

SECTION 1. 100.75 of the statutes is created to read:

100.75 Requirements and standards for the sharing of sensitive information between separate legal entities. (1) DEFINITIONS. In this section:

(a) "Data" includes sensitive information, such as personally identifiable information and nonpublic or privately held information, and nonsensitive information, such as public information or deidentified personal information.

(b) "Data agreement" means a written data contract entered into between data controllers. "Data agreement" includes any of the following:

1. Data sharing agreements establishing terms for a data custodian providing storage of data owned by a data owner.

2. Data use agreements establishing terms for a data steward using data owned by a data owner for a specific mutually agreed–upon purpose.

3. Data access agreements establishing terms for a data steward using data owned by a data owner and housed within a data custodian's data storage environment.

(c) "Data controller" means any entity, public or private, that determines the purposes and means of processing data, and that is responsible for complying with applicable data protection laws and ensuring that data is handled in a lawful and responsible manner. "Data controller" includes data custodians, data owners, and data stewards.

(d) "Data custodian" means any person that provides data storage on behalf of a data owner.

(e) "Data owner" means any person that generates, collects, or uses data for its own purposes.

(f) "Data steward" means any person that uses or facilitates the use of data on behalf of a data owner.

(g) "Deidentified personal information" means information that cannot reasonably be linked to an identified person, identifiable person, or device linked to a person. "Deidentified personal information" includes aggregated information, generalized information, and randomized information.

(h) "Enhanced data" means data that has been standardized, derived, aggregated, organized, corrected, verified, augmented, merged with other data, or otherwise prepared for further analysis or use. "Enhanced data" may be based on data from more than one data owner.

(i) "Metadata" means data that describes other data.

(j) "Nonpublic or privately held information" means information that is not publicly available or accessible to the general public; is restricted to a specific group of individuals or entities; is considered confidential or proprietary; is protected by privacy regulations; and requires appropriate safeguards to prevent unauthorized access, use, or disclosure. "Nonpublic or privately held information" includes intellectual property, financial information, confidential business agreements, and regulatory information.

(k) "Nonsensitive information" means information that is not subject to legal protections due to its nature or potential impact on individuals' privacy, security, or other rights. "Nonsensitive information" includes public information and deidentified personal information.

(L) "Personally identifiable information" means information that is or can reasonably be linked to an identified person, identifiable person, or device linked to a person. "Personally identifiable information" includes identifying attributes, contact information, personal characteristics, financial information, biometric data, health and medical information, online identifiers, and education and employment information.

(m) "Public information" means information that is lawfully made available through federal, state, or local government records, or information that is reasonably believed to be lawfully made available to the general public through widely

distributed media by the consumer or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.

(n) "Sensitive information" means any type of information that, if disclosed or accessed by unauthorized parties, could result in harm, privacy violations, or negative consequences for individuals or entities. "Sensitive information" includes information that requires special protection due to its nature and includes personally identifiable information and nonpublic or privately held information. "Sensitive information" includes nonsensitive information that is mingled with sensitive information.

(2) REQUIREMENTS FOR DATA CONTROLLERS. (a) A data owner that generates, collects, or uses sensitive information shall do all of the following:

1. Limit the access to, sharing of, and use of its data to what is adequate, relevant, and reasonably necessary for the purposes for which the data is collected or generated.

2. Establish and ensure compliance with internal policies and procedures governing the review of data sharing and data use requests. Such policies and procedures shall include all of the following:

a. A schedule indicating how often the data owner will review requests.

b. Assessment criteria for the approval or rejection of requests.

c. Documentation of the rationale for the rejection of a request.

d. Notice of the rejection to the requesting entity.

3. Establish and ensure compliance with internal policies and with any relevant regulatory requirements on the sharing of sensitive information with another legal entity.

4. Establish and ensure compliance with internal policies and procedures that reflect best practices of data handling on all of the following subjects:

a. Identity and access management controls, including limiting the access to any data subject to a data agreement.

b. Data retention and data destruction.

c. The periodic review of new and changing business and regulatory requirements that may impact data sharing.

5. Establish and ensure compliance with internal policies and procedures regarding the handling of data agreement breaches; security incidents, in compliance with s. 134.98; and related disputes.

(b) A data custodian that provides storage for sensitive information shall do all of the following:

1. Provide a secure environment for the storage of a data owner's data. The environment shall be designed and configured in a manner that reflects best practices of data security on subjects including all of the following:

a. Identity and access management controls, including limiting the access to any data subject to a data agreement.

b. Role–based permissions, including limiting the access to data subject to a data agreement to only authorized users.

c. Data encryption at rest and in transit.

d. Cyber security monitoring and threat detection.

e. Recovery capabilities in the event of a disaster, such as fail–over, backup, and restore capabilities.

2. Establish and ensure compliance with internal policies and procedures that reflect best practices on all of the following subjects:

a. Data access control.

b. Data retention and data destruction.

c. Auditing capabilities and the performance of audits.

d. The periodic review of new and changing business and regulatory requirements that may impact data solution organization.

e. Any other requirements established in a data agreement.

3. Establish and ensure compliance with internal policies and procedures related to security incidents that include all of the following:

a. A description of the severity levels by which security incidents are classified with descriptions and relevant examples for each severity classification.

b. The number of hours after a security incident is detected when a data custodian must notify the data owner and data steward of the incident and the timing of subsequent updates, based on the nature or severity of the incident.

c. A policy and process to designate a specific member of the data custodian's team to provide security incident communications to the data owner and data steward.

d. A policy to inform the data owner and data steward of the time the incident occurred, if known; the time the incident was detected; the nature of the incident, including which data sets were known to have been impacted; the severity of the incident; the remediation steps that have been or will be taken; the estimated timeline to resolve the incident; and a way for the data owner or data steward to contact the data custodian to seek further information about the incident.

e. A policy to provide a follow–up notification after the resolution of an incident that includes the time the incident was resolved, the nature of the resolution, any changes to the data custodian's systems or protocols to prevent subsequent incidents,

and any recommended changes to the data owner's or data steward's systems protocols to prevent subsequent incidents.

f. A record retention policy that requires the data custodian to maintain records detailing its response to security incidents for a reasonable time after the resolution of the security incident.

4. Establish and ensure compliance with internal policies and procedures related to auditing capabilities that require the data custodian to perform an audit of its systems at the request of the data owner.

(c) A data steward that uses or facilitates the use of sensitive information shall do all of the following:

1. Establish and ensure compliance with internal policies and procedures that reflect best practices of data handling on subjects including all of the following:

a. Standards, policies, procedures, and requirements for requesting, accessing, interpreting, and using data.

b. Identity and access management controls, including limiting the access to any data subject to a data agreement.

c. Verification of data outputs to meet quality, accuracy, and reliability specifications.

d. Establishment of data element definitions and lineage.

e. Establishment and maintenance of auditing policies, procedures, and reporting.

f. Policies and procedures regarding data retention and destruction.

g. Interpretation of new and changing business and regulatory requirements that may impact data solution organization.

h. Any other requirements established in a data agreement.

2. Establish and ensure compliance with policies and procedures regarding the handling of data agreement breaches, security incidents, in compliance with s. 134.98, and related disputes.

(3) AGREEMENTS BETWEEN DATA CONTROLLERS. Data agreements are required when sensitive information controlled by one data controller is to be shared with, accessed by, or used by another data controller. A data agreement shall contain all of the following provisions:

(a) Identification of the parties to the agreement.

(b) Identification of the data subject to the agreement.

(c) Identification of the permitted uses and restrictions of the data subject to the agreement, including whether the data owner permits the data controller to share with another entity any enhanced data that was based on the data owner's original data.

(d) Identification of any confidentiality requirements for the data subject to the agreement.

(e) Identification of the law governing the data subject to the agreement, such as the federal Family Educational Rights and Privacy Act, the federal Health Insurance Portability and Accountability Act, the federal Health Information Technology for Economic and Clinical Health Act, the federal Criminal Justice Information Services Security Policy, or the federal Children's Online Privacy Protection Rule.

(f) Identification of the governing law and venue that shall govern the validity, construction, enforcement, and interpretation of the agreement.

(g) Provisions governing the response to security incidents, in compliance with s. 134.98, including all of the following:

1. The name and contact information of one or more individuals who are authorized to provide and receive security incident communications pertaining to the data subject to the agreement.

2. An attestation from a data custodian that it has established and agrees to comply with security incident policies and procedures under sub. (2) (b) 3.

(h) Definition of the term of the data agreement. A data agreement under this section shall remain in effect until a mutually agreed upon termination date or until all data subject to the agreement is destroyed or returned to the data owner, whichever occurs first.

(i) Provisions regarding the right to terminate the agreement, including all of the following:

1. Conditions under which the agreement may be terminated.

2. The method of notification required before termination is effective.

3. The advance notice period required before termination is effective.

4. Any special circumstances under which immediate termination of the agreement may be pursued.

(j) Provisions regarding authorization for or prohibition of the collection and analysis of metadata.

(k) In a data sharing agreement between a data owner and a data custodian, provisions regarding auditing capabilities and the performance of audits. A data custodian shall attest that it has enabled appropriate capabilities to support compliance with the regulatory statutes identified in the agreement and shall agree, at the request of the data owner, to perform an audit of the data owner's data under its custodianship. Such an audit shall have a mutually agreed upon scope and shall be performed within a mutually agreed upon time frame.

(L) Any other requirements as established by any party to the agreement.

(END)