State of Wisconsin
2019 - 2020 LEGISLATURE

LRB-4120/1
KP:ahe&amn

2019 ASSEMBLY BILL 870

February 10, 2020 – Introduced by Representatives ZIMMERMAN, WITTKE, QUINN, DUCHOW, WICHGERS, PLUMER, SORTWELL, KULP, THIESFELDT, KNODL, GUNDRUM, BROSTOFF, MACCO and STEFFEN, cosponsored by Senator RISSER. Referred to Committee on Science and Technology.

AUTHORS SUBJECT TO CHANGE

AN ACT ***to create*** 134.985 of the statutes; **relating to:** consumer access to personal data processed by a controller and providing a penalty.

Analysis by the Legislative Reference Bureau

This bill generally requires controllers of consumers' personal data to provide a consumer with copies of the consumer's personal data processed by the controller.

Under the bill, a "controller" is a person that alone or jointly with others determines the purposes and means of the processing of personal data. The bill defines "personal data" as information relating to a consumer that allows the consumer to be identified other than information lawfully made available from federal, state, or local government records.

The bill requires a controller, when collecting personal data from a consumer, to inform the consumer that it is collecting personal data and to provide the consumer with certain other information. Additionally, if a controller intends to process a consumer's personal data and the controller did not collect the personal data from the consumer, the controller must, within one month of obtaining the personal data, identify itself to the consumer and provide the consumer with certain information, such as the purposes for which the controller intends to process the personal data and where the controller obtained the personal data.

Also, under the bill, if a controller processes a consumer's personal data, the controller must provide a copy of the personal data to a consumer who requests a copy. The controller must also provide the consumer with certain other information, including the purposes for which the controller processes the personal data, the categories of the personal data that the controller processes, and the persons to

whom the controller discloses the personal data. If a consumer requests a copy of personal data electronically, the controller must provide the copy and requested information in a commonly used electronic form, unless the consumer requests otherwise. A controller is not required to provide a consumer with a copy of the consumer's personal data 1) if providing the copy would adversely affect the rights of others; 2) if the controller processes a consumer's personal data out of necessity in performing a task for the public interest; or 3) if the personal data is certain health, financial, or other personal information, including information restricted by federal law.

The bill also requires a controller to notify the Department of Justice if the controller is aware of a personal data breach involving consumer personal data it maintains and the data breach is likely to result in a risk to the rights and freedoms of consumers. The notification must describe the nature of the personal data breach and provide certain additional information. Also, if the personal data breach is likely to result in a high risk to the rights and freedoms of consumers, a controller generally must notify the consumers whose personal data is involved in the personal data breach. The bill also requires a processor to notify a controller about a personal data breach of personal data that it maintains on behalf of the controller.

Under the bill, the attorney general may investigate violations and bring actions for enforcement. A controller who violates the bill's personal data breach notification requirements is subject to a fine of up to $10,000,000 or up to 2 percent of the controller's total annual revenue, whichever is greater. For violating the bill's requirements related to providing copies of a consumer's personal data, a controller may be fined up to $20,000,000 or up to 4 percent of the controller's total annual revenue, whichever is greater.

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

SECTION 1. 134.985 of the statutes is created to read:

134.985 Access to personal data. (1) DEFINITIONS. In this section:

(a) "Consumer" means an individual who is a resident of this state.

(b) "Controller" means a person that alone or jointly with others determines the purposes and means of the processing of personal data, but does not include a law enforcement agency or a unit or instrumentality of the federal government, the state, or a local government.

(c) "Personal data" means information relating to an consumer that allows the consumer to be identified, either directly or indirectly, including by reference to an identifier such as a name, identification number, location data, online identifier, or one or more factors related to the physical, physiological, genetic, mental, economic, cultural, or social identity of the consumer, but does not include any information lawfully made available from federal, state, or local government records.

(d) "Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

(e) "Process," when used in reference to personal data, means to perform an operation or set of operations on personal data, including to collect, record, organize, store, alter, retrieve, use, disclose, disseminate, make available, combine, delete, or destroy the personal data.

(f) "Processor" means a person who processes personal data on behalf of a controller, but does not include a law enforcement agency or a unit or instrumentality of the federal government, the state, or a local government.

(g) "Recipient" means a person to which personal data is disclosed.

(2) NOTICE REQUIRED. (a) Except as provided in par. (b), at the time when a controller collects personal data from a consumer, the controller shall provide the consumer with the following information:

1. The identity and contact information of the controller.

2. The purposes for which the controller intends to process the consumer's personal data and the legal authority for conducting the processing.

3. The recipients or categories of recipients to whom the consumer's personal data will be disclosed.

4. If known, the estimated period of time that the controller will store the consumer's personal data, or, if not known, the criteria the controller will use to determine the amount of time that the controller will store the personal data.

5. Information describing the consumer's ability to make requests under sub. (3).

6. Whether the controller will use the consumer's personal data to conduct automated decision–making related to the consumer, and, if so, the purpose for which automated decision–making will be used and meaningful information about the automated decision–making procedure.

(b) A controller is not required to provide a consumer with information under par. (a) if the consumer has previously been provided with the information required under par. (a).

(c) Except as provided in par. (d), if a controller intends to process a consumer's personal data and the controller did not collect the personal data from the consumer, within one month of obtaining the personal data, the controller shall provide the consumer with the following information:

1. The identity and contact information of the controller.

2. The purposes for which the controller intends to process the consumer's personal data and the legal authority for conducting the processing.

3. The categories of the consumer's personal data that the controller intends to process.

4. The recipients or categories of recipients to whom the consumer's personal data will be disclosed.

5. If known, the estimated period of time that the controller will store the consumer's personal data, or, if not known, the criteria the controller will use to determine the amount of time that the controller will store the personal data.

6. Information describing the consumer's ability to make requests under sub. (3).

7. The controller's source for the personal data, including whether the personal data was obtained from publicly accessible sources.

8. Whether the controller will use the consumer's personal data to conduct automated decision–making related to the consumer, and, if so, the purpose for which automated decision–making will be used and meaningful information about the automated decision–making procedure.

(d) A controller is not required to provide a consumer with information under par. (c) if any of the following applies:

1. The consumer has previously been provided with the information required under par. (c).

2. Providing the information is impossible or involves unreasonable effort.

3. Federal, state, or local law requires that the information not be disclosed.

(3) ACCESS TO PERSONAL DATA. (a) Upon a consumer's request, a controller shall inform the consumer as to whether or not the controller processes the consumer's personal data.

(b) 1. If a controller processes a consumer's personal data, upon the consumer's request, the controller shall provide the consumer with a copy of the consumer's personal data and all of the following information:

a. The purposes for which the controller processes the consumer's personal data.

b. The categories of the consumer's personal data that the controller processes.

c. The recipients or categories of recipients to whom the consumer's personal data have been or will be disclosed.

d. If known, the estimated period of time that the controller will store the consumer's personal data, or, if not known, the criteria the controller will use to determine the amount of time that the controller will store the personal data.

e. If the controller did not collect the personal data from the consumer, any available information on the controller's source for the personal data.

2. If the consumer makes a request under this paragraph to the controller by electronic means, the controller shall provide the information required under subd. 1. to the consumer in a commonly used electronic form, unless otherwise requested by the consumer.

3. a. Except as provided in subd. 3. b., a controller shall provide copies and information required under subd. 1. free of charge.

b. If a request from a consumer is manifestly unfounded or excessive, including by being repetitive, a controller may either charge the consumer a reasonable fee based on the administrative costs of providing a copy or information or refuse to act on the request. The controller bears the burden of demonstrating the a consumer's request is manifestly unfounded or excessive.

4. a. Except as provided in subd. 4. b., a controller shall provide a copy and information under subd. 1. within one month of receiving a consumer's request.

b. A controller may provide a copy and information under subd. 1. within 3 months of receiving a consumer's request if necessary due to the complexity and number of requests received by the controller. If the controller does not provide a copy and information under subd. 1. to a consumer within one month of the

consumer's request, the controller shall within one month of the consumer's request inform the consumer about the delay and notify the consumer of the reason for the delay.

5. A controller is not required to provide a consumer with a copy and information under subd. 1. if any of the following applies:

a. The controller processes the consumer's personal data out of necessity for performing a task carried out in the public interest or out of necessity for exercising official authority vested in the controller.

b. Providing a copy would adversely affect the rights of others.

(c) This subsection does not require a controller to do any of the following:

1. Reidentify data that does not identify a consumer.

2. Retain, link, or combine personal data concerning a consumer that the controller would not otherwise retain, link, or combine in its ordinary course of business.

3. Comply with a request under this subsection if the controller is unable to verify, using commercially reasonable efforts, the identity of the consumer making the request.

(4) PERSONAL DATA BREACH NOTIFICATION. (a) 1. Except as provided in subd. 2., if a controller is aware of a personal data breach of personal data maintained by the controller, the controller shall notify the department of justice of the personal data breach without undue delay. If feasible, the controller shall notify the department within 30 days of becoming aware of the personal data breach. If the controller does not notify the department within 30 days of becoming aware of the personal data breach, the controller shall provide a reason for not notifying within 30 days. The notification shall do all of the following:

a. Describe the nature of the personal data breach including, if known, the categories and approximate number of consumers involved and the categories and approximate number of personal data records involved.

b. Describe the likely consequences of the personal data breach.

c. Describe the measures taken or proposed by the controller to address the personal data breach, including, if appropriate, measures to mitigate the possible adverse effects.

2. A controller is not required to make a notification under this paragraph if the personal data breach is unlikely to result in a risk to the rights and freedoms of consumers.

3. If it is not possible to provide the information required under subd. 1. at the same time, the controller may provide the information in stages without undue delay.

4. If a processor is aware of a personal data breach of personal data that the processor maintains on behalf of a controller, the processor shall notify the controller without undue delay.

(b) 1. Except as provided in subd. 2., if a controller is aware of a personal data breach of personal data maintained by the controller and the personal data breach is likely to result in a high risk to the rights and freedoms of consumers, the controller shall notify the consumers whose personal data is involved in the personal data breach. The notification shall describe in clear and plain language the nature of the personal data breach and contain the information described in par. (a) 1. b. and c.

2. A controller is not required to make a notification under this paragraph if any of the following applies:

a. The controller has implemented appropriate technical and organizational protection measures to the personal data involved in the personal data breach that

render the personal data unintelligible to any person who is not authorized to access it.

b. The controller takes measures after the personal data breach that ensure that a high risk to the rights and freedoms of consumers is not likely to exist.

c. Making the notification involves unreasonable effort. If this subd. 2. c. applies, the controller shall publicly communicate about the personal data breach to consumers in an effective manner.

(5) APPLICABILITY. (a) This section does not require a controller to confirm processing or provide a copy of the following types of information:

1. Health information protected by the federal Health Insurance Portability and Accountability Act of 1996.

2. Information identifying a patient covered by 42 USC 290dd–2.

3. Information collected as part of research subject to the Federal Policy for the Protection of Human Subjects, 45 CFR part 46, or subject to 21 CFR parts 50 and 56.

4. Information and documents created specifically for and collected and maintained by a hospital.

5. Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986, 42 USC 11101 et seq.

6. Patient safety work product information for purposes of 42 USC 299b–21 to 299b–26.

7. Information maintained by a health care provider, a health care facility, or an entity covered by the federal Health Insurance Portability and Accountability Act of 1996.

8. Personal information provided to or from or held by a consumer reporting agency, as defined in s. 422.501 (1m), if the use of the information complies with the federal Fair Credit Reporting Act, 15 USC 1681 et seq.

9. Personal information collected, processed, sold, or disclosed pursuant to the federal Gramm–Leach–Bliley Act, P.L. 106–102.

10. Personal information collected, processed, sold, or disclosed pursuant to the federal Driver's Privacy Protection Act, 18 USC 2721 et seq.

11. Information maintained for employment records.

(b) This section does not apply to a consumer who processes personal data in connection with a purely personal or household activity.

(c) This section does not apply to a controller that processes a consumer's personal data for literary or artistic purposes.

(d) This section does not apply to a controller that processes a consumer's personal data, that intends to publish the personal data, and that believes that publication of the personal data is in the public interest.

(6) ENFORCEMENT; PENALTIES. (a) The attorney general may investigate violations of this section and may bring actions for enforcement of this section.

(b) 1. A controller who violates sub. (4) shall be fined not more than $10,000,000 or not more than 2 percent of the controller's total annual revenue during the preceding financial year, whichever is greater.

2. A controller who violates sub. (2) or (3) shall be fined not more than $20,000,000 or not more than 4 percent of the controller's total annual revenue during the preceding financial year, whichever is greater.

3. A court may not impose in the same action more than one fine on a controller under this paragraph unless the additional fine is imposed for a violation that does not involve the same or linked processing activities by the controller.

SECTION 2. Effective date.

(1) This act takes effect on July 31, 2022.

(END)