



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.

1 **AN ACT** *to create* 134.985 of the statutes; **relating to:** consumer access to
2 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

ASSEMBLY BILL 870

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:

- 1 **SECTION 1.** 134.985 of the statutes is created to read:
- 2 **134.985 Access to personal data. (1) DEFINITIONS.** In this section:
- 3 (a) "Consumer" means an individual who is a resident of this state.
- 4 (b) "Controller" means a person that alone or jointly with others determines the
- 5 purposes and means of the processing of personal data, but does not include a law
- 6 enforcement agency or a unit or instrumentality of the federal government, the state,
- 7 or a local government.

ASSEMBLY BILL 870

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

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

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

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

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

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

21 1. The identity and contact information of the controller.

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

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

ASSEMBLY BILL 870**SECTION 1**

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

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

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

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

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

17 1. The identity and contact information of the controller.

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

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

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

ASSEMBLY BILL 870

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

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

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

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

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

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

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

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

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

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

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

ASSEMBLY BILL 870**SECTION 1**

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

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

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

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

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

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

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

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

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

ASSEMBLY BILL 870

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

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

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

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

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

11 1. Reidentify data that does not identify a consumer.

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

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

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

ASSEMBLY BILL 870**SECTION 1**

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

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

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

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

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

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

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

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

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

ASSEMBLY BILL 870

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

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

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

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

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

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

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

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

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

19 6. Patient safety work product information for purposes of 42 USC 299b-21 to
20 299b-26.

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

ASSEMBLY BILL 870**SECTION 1**

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

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

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

8 11. Information maintained for employment records.

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

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

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

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

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

21 2. A controller who violates sub. (2) or (3) shall be fined not more than
22 \$20,000,000 or not more than 4 percent of the controller's total annual revenue
23 during the preceding financial year, whichever is greater.

