



State of Wisconsin  
2019 - 2020 LEGISLATURE

LRB-4120/P2 *sep3*  
KP:ahet *amv*

**PRELIMINARY DRAFT - NOT READY FOR INTRODUCTION**

*INSERT*

*IN: 9/18/2019*  
*OUT: 9/19/2019*

*Regen.*

- 1 **AN ACT to create** 100.71 of the statutes; **relating to:** consumer access to personal
- 2 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.

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 Agriculture, Trade and Consumer Protection 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.

*e Justice*

*INS A*

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

1 *134.985* SECTION 1. 100.71 of the statutes is created to read:

2 100.71 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 unit  
6 or instrumentality of the federal government, the state, or a local government.

7 (c) "Personal data" means information relating to an consumer that allows the  
8 consumer to be identified, either directly or indirectly, including by reference to an  
9 identifier such as a name, identification number, location data, online identifier, or  
10 one or more factors related to the physical, physiological, genetic, mental, economic,  
11 cultural, or social identity of the consumer.

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

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

8 (f) "Processor" means a person who processes personal data on behalf of a  
9 controller.

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

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

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

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

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

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

22 5. Information describing the consumer's ability to make requests under sub.

23 (3).

24 6. Whether the controller will use the consumer's personal data to conduct  
25 automated decision-making related to the consumer, and, if so, the purpose for

1 which automated decision-making will be used and meaningful information about  
2 the automated decision-making procedure.

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

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

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

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

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

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

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

20 6. Information describing the consumer's ability to make requests under sub.  
21 (3).

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

24 8. Whether the controller will use the consumer's personal data to conduct  
25 automated decision-making related to the consumer, and, if so, the purpose for

1 which automated decision-making will be used and meaningful information about  
2 the automated decision-making procedure.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14          b. A controller may provide a copy and information under subd. 1. within 3  
15 months of receiving a consumer's request if necessary due to the complexity and  
16 number of requests received by the controller. If the controller does not provide a  
17 copy and information under subd. 1. to a consumer within one month of the  
18 consumer's request, the controller shall within one month of the consumer's request  
19 inform the consumer about the delay and notify the consumer of the reason for the  
20 delay.

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

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

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

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

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

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

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

10 (4) PERSONAL DATA BREACH NOTIFICATION. (a) 1. Except as provided in subd. 2.,  
11 if a controller is aware of a personal data breach of personal data maintained by the  
12 controller, the controller shall notify the department <sup>of justice</sup> of the personal data breach  
13 without undue delay. If feasible, the controller shall notify the department within  
14 72 hours of becoming aware of the personal data breach. If the controller does not  
15 notify the department within 72 hours of becoming aware of the personal data  
16 breach, the controller shall provide a reason for not notifying within 72 hours. The  
17 notification shall do all of the following:

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

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

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

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

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

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

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

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

17           a. The controller has implemented appropriate technical and organizational  
18 protection measures to the personal data involved in the personal data breach that  
19 render the personal data unintelligible to any person who is not authorized to access  
20 it.

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

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



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

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

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

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

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

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

12          6. Patient safety work product information for purposes of 42 USC 299b-21 to  
13 299b-26.

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

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

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

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

24          11. Information maintained for employment records.

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

*INS 10-2 n*

3 **SECTION 2. Effective date.**

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

5 (END)

2019-2020 DRAFTING INSERT  
FROM THE  
LEGISLATIVE REFERENCE BUREAU

LRB-4120/P3ins  
KP:... *Ann*

1 INS A

A person injured because of a violation of the bill may bring a civil action for damages. Also, 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.

2

3 END INS A

4 INS 10-2

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

*processes*

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

10 (6) PRIVATE ACTION. In addition to any other remedies, a person injured because  
11 of a violation of this section by another person may bring a civil action for damages  
12 in any circuit court.

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

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

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

4           END INS 10-2



State of Wisconsin  
2019 - 2020 LEGISLATURE

LRB-4120/P3  
KP:ahe&amn

**PRELIMINARY DRAFT - NOT READY FOR INTRODUCTION**

IN: 10/2/2019  
OUT: 10/3/2019

- 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.

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.

A person injured because of a violation of the bill may bring a civil action for damages. Also, 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 unit
- 6 or instrumentality of the federal government, the state, or a local government.
- 7           (c) "Personal data" means information relating to an consumer that allows the
- 8 consumer to be identified, either directly or indirectly, including by reference to an

1 identifier such as a name, identification number, location data, online identifier, or  
2 one or more factors related to the physical, physiological, genetic, mental, economic,  
3 cultural, or social identity of the consumer.

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

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

11 (f) "Processor" means a person who processes personal data on behalf of a  
12 controller.

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

14 **(2) NOTICE REQUIRED.** (a) Except as provided in par. (b), at the time when a  
15 controller collects personal data from a consumer, 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 recipients or categories of recipients to whom the consumer's personal  
21 data will be disclosed.

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

1           5. Information describing the consumer's ability to make requests under sub.  
2 (3).

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

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

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

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

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

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

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

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

24           6. Information describing the consumer's ability to make requests under sub.  
25 (3).



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

19           b. A controller may provide a copy and information under subd. 1. within 3  
20 months of receiving a consumer's request if necessary due to the complexity and  
21 number of requests received by the controller. If the controller does not provide a  
22 copy and information under subd. 1. to a consumer within one month of the  
23 consumer's request, the controller shall within one month of the consumer's request  
24 inform the consumer about the delay and notify the consumer of the reason for the  
25 delay.

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

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

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

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

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

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

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

15           **(4) PERSONAL DATA BREACH NOTIFICATION.** (a) 1. Except as provided in subd. 2.,  
16 if a controller is aware of a personal data breach of personal data maintained by the  
17 controller, the controller shall notify the department of justice of the personal data  
18 breach without undue delay. If feasible, the controller shall notify the department  
19 within 72 hours of becoming aware of the personal data breach. If the controller does  
20 not notify the department within 72 hours of becoming aware of the personal data  
21 breach, the controller shall provide a reason for not notifying within 72 hours. The  
22 notification shall do all of the following:

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

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

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

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

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

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

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

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

21          a. The controller has implemented appropriate technical and organizational  
22 protection measures to the personal data involved in the personal data breach that  
23 render the personal data unintelligible to any person who is not authorized to access  
24 it.

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

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

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

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

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

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

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

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

17           6. Patient safety work product information for purposes of 42 USC 299b-21 to  
18 299b-26.

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

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

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

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

5 11. Information maintained for employment records.

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

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

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

13 (6) PRIVATE ACTION. In addition to any other remedies, a person injured because  
14 of a violation of this section by another person may bring a civil action for damages  
15 in any circuit court.

16 (7) 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.

24 **SECTION 2. Effective date.** *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.*





State of Wisconsin  
2019 - 2020 LEGISLATURE

LRB-4120/P4 *eps*  
KP:ahe&amn

**PRELIMINARY DRAFT - NOT READY FOR INTRODUCTION**

*IN: 10/30*  
*OUT: 10/31*

*so ✓*

- 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 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.

A person injured because of a violation of the bill may bring a civil action for damages. Also, 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 unit  
6 or instrumentality of the federal government, the state, or a local government.

7           (c) "Personal data" means information relating to an consumer that allows the  
8 consumer to be identified, either directly or indirectly, including by reference to an

1 identifier such as a name, identification number, location data, online identifier, or  
2 one or more factors related to the physical, physiological, genetic, mental, economic,  
3 cultural, or social identity of the consumer. *, but does not include any information lawfully made available from  
federal, state, or local government records*

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

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

11 (f) "Processor" means a person who processes personal data on behalf of a  
12 controller.

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

14 (2) NOTICE REQUIRED. (a) Except as provided in par. (b), at the time when a  
15 controller collects personal data from a consumer, 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 recipients or categories of recipients to whom the consumer's personal  
21 data will be disclosed.
- 22 4. If known, the estimated period of time that the controller will store the  
23 consumer's personal data, or, if not known, the criteria the controller will use to  
24 determine the amount of time that the controller will store the personal data.

1           5. Information describing the consumer's ability to make requests under sub.  
2           (3).

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

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

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

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

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

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

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

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

24           6. Information describing the consumer's ability to make requests under sub.  
25          (3).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

19 b. A controller may provide a copy and information under subd. 1. within 3  
20 months of receiving a consumer's request if necessary due to the complexity and  
21 number of requests received by the controller. If the controller does not provide a  
22 copy and information under subd. 1. to a consumer within one month of the  
23 consumer's request, the controller shall within one month of the consumer's request  
24 inform the consumer about the delay and notify the consumer of the reason for the  
25 delay.

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

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

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

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

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

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

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

15           **(4) PERSONAL DATA BREACH NOTIFICATION.** (a) 1. Except as provided in subd. 2.,  
16 if a controller is aware of a personal data breach of personal data maintained by the  
17 controller, the controller shall notify the department of justice of the personal data  
18 breach without undue delay. If feasible, the controller shall notify the department  
19 within 72 hours of becoming aware of the personal data breach. If the controller does  
20 not notify the department within 72 hours of becoming aware of the personal data  
21 breach, the controller shall provide a reason for not notifying within 72 hours. The  
22 notification shall do all of the following:

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

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

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

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

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

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

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

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

21           a. The controller has implemented appropriate technical and organizational  
22 protection measures to the personal data involved in the personal data breach that  
23 render the personal data unintelligible to any person who is not authorized to access  
24 it.

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

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

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

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

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

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

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

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

17           6. Patient safety work product information for purposes of 42 USC 299b-21 to  
18 299b-26.

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

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



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

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

5 11. Information maintained for employment records.

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

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

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

13 (6) PRIVATE ACTION. In addition to any other remedies, a person injured because  
14 of a violation of this section by another person may bring a civil action for damages  
15 in any circuit court.

16 (6) (7) 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.



## Paczuski, Konrad

---

**From:** Augustyn, Ryan <Ryan.Augustyn@legis.wisconsin.gov>  
**Sent:** Wednesday, October 30, 2019 10:39 AM  
**To:** Paczuski, Konrad <Konrad.Paczuski@legis.wisconsin.gov>  
**Subject:** Update to Data Bills

Hi Konrad,

The representative has a few changes for the bills to update into a p5. They are:

- Remove private right of action for enforcement (so right now only AG action would be used).
- Exclude from the definition of 'personal information' public records. We can define public records as: information that is lawfully made available from federal, state, or local government records
- Record keeping: I checked into an example of GDPR record keeping, and it can be very extensive. Explicitly laying out categories may help lower the record keeping burden, especially on small business. I'm not sure how to put this in the bill, but record keeping will be about categories of data and processing, not each individual instance (say if you double check someone's address in your system, we don't want to have two records of processing data, more generally that this data is accessed for billing purposes). So in addition to the controller contact information, the categories of personal data types involved in the processing, we would require the purpose of processing, name and contact information of third parties data transferred to, purpose of transferring data to third party, and link to record of consent.
- In LRB 4122 on page 6, line 6 delete 'or trade union purpose'.
- In LRB 4122, on page 6 delete lines 19-21 and just replace with something like 'processing the personal data is necessary for the purpose of providing health care or treatment when a person is having a medical emergency'.

Question: in LRB 4121 (deletion), does the non-profit exemption have to be replicated from the processing bill? It looks like the bills currently allow nonprofits of political, philosophical, or religious persuasion to process, but anyone can delete. We would like to exempt entities that fall under those categories so please change if necessary.

You answered my question on the health information otherwise. As always, thank you for your work on this,

Ryan Augustyn  
Office of Representative Shannon Zimmerman  
(608) 266-1526



Additional instructions from Rep. Zimmerman's office:

- Change the breach notification deadline requirement from 72 hours to 30 days.
- Include a provision that explicitly exempts law enforcement agencies from the draft.



State of Wisconsin  
2019 - 2020 LEGISLATURE

LRB-4120/P5 *De P6*  
KP:ahe&amn

**PRELIMINARY DRAFT - NOT READY FOR INTRODUCTION**

*IN: 12/30/2019*  
*OUT: 1/3/2020*

*sa<sup>v</sup>*

- 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

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 <sup>a law enforcement agency or</sup> a unit  
 6           or instrumentality of the federal government, the state, or a local government.

7           (c) "Personal data" means information relating to an consumer that allows the  
 8           consumer to be identified, either directly or indirectly, including by reference to an

1 identifier such as a name, identification number, location data, online identifier, or  
2 one or more factors related to the physical, physiological, genetic, mental, economic,  
3 cultural, or social identity of the consumer, but does not include any information  
4 lawfully made available from federal, state, or local government records.

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

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

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

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

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

- 18 1. The identity and contact information of the controller.
- 19 2. The purposes for which the controller intends to process the consumer's  
20 personal data and the legal authority for conducting the processing.
- 21 3. The recipients or categories of recipients to whom the consumer's personal  
22 data will be disclosed.
- 23 4. If known, the estimated period of time that the controller will store the  
24 consumer's personal data, or, if not known, the criteria the controller will use to  
25 determine the amount of time that the controller will store the personal data.

1           5. Information describing the consumer's ability to make requests under sub.  
2 (3).

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

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

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

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

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

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

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

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

24           6. Information describing the consumer's ability to make requests under sub.  
25 (3).



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

19          b. A controller may provide a copy and information under subd. 1. within 3  
20 months of receiving a consumer's request if necessary due to the complexity and  
21 number of requests received by the controller. If the controller does not provide a  
22 copy and information under subd. 1. to a consumer within one month of the  
23 consumer's request, the controller shall within one month of the consumer's request  
24 inform the consumer about the delay and notify the consumer of the reason for the  
25 delay.

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

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

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

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

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

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

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

15           (4) PERSONAL DATA BREACH NOTIFICATION. (a) 1. Except as provided in subd. 2.,  
16 if a controller is aware of a personal data breach of personal data maintained by the  
17 controller, the controller shall notify the department of justice of the personal data  
18 breach without undue delay. If feasible, the controller shall notify the department  
19 within 72 hours of becoming aware of the personal data breach. If the controller does  
20 not notify the department within 72 hours of becoming aware of the personal data  
21 breach, the controller shall provide a reason for not notifying within 72 hours. The  
22 notification shall do all of the following:

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

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

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

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

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

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

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

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

21           a. The controller has implemented appropriate technical and organizational  
22 protection measures to the personal data involved in the personal data breach that  
23 render the personal data unintelligible to any person who is not authorized to access  
24 it.

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

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

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

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

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

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

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

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

17           6. Patient safety work product information for purposes of 42 USC 299b-21 to  
18 299b-26.

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

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

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

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

5           11. Information maintained for employment records.

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

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

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

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

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

18          2. A controller who violates sub. (2) or (3) shall be fined not more than  
19 \$20,000,000 or not more than 4 percent of the controller's total annual revenue  
20 during the preceding financial year, whichever is greater.

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

24          **SECTION 2. Effective date.**



## Walker, Dan

---

**From:** Paczuski, Konrad  
**Sent:** Thursday, January 23, 2020 2:48 PM  
**To:** Walker, Dan  
**Subject:** -4120, -4121, -4122

Dan,

I have redrafted -4120, -4121, and -4122 into introducible versions. Could you please pull those files and submit jacketed versions of each of those drafts?

Thanks,  
Konrad





State of Wisconsin  
2019 - 2020 LEGISLATURE

LRB-4120/P6  
KP:ah&amn

1

No  
Change

**PRELIMINARY DRAFT - NOT READY FOR INTRODUCTION**

- 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



**Walker, Dan**

---

**From:** LRB.Legal  
**To:** Rep.Zimmerman  
**Subject:** Draft review: LRB -4120/1  
**Attachments:** 19-4120/1

**State of Wisconsin - Legislative Reference Bureau**  
**One East Main Street - Suite 200 - Madison**

**The attached draft was prepared at your request. Please review it carefully to ensure that it satisfies your intent.** If you have any questions concerning the draft or would like to have it redrafted, please contact Konrad Paczuski, Legislative Attorney, at (608) 504-5814, at [Konrad.Paczuski@legis.wisconsin.gov](mailto:Konrad.Paczuski@legis.wisconsin.gov), or at One East Main Street, Suite 200.

**We will jacket this draft for introduction in the Assembly.**

**If a jacket is needed immediately, please let us know in your response e-mail so we know to immediately jacket the proposal for you.**

If the last paragraph of the analysis states that a fiscal estimate will be prepared, the LRB will submit a request to DOA when the draft is introduced. You may obtain a fiscal estimate on the draft prior to introduction by contacting our program assistants at [LRB.Legal@legis.wisconsin.gov](mailto:LRB.Legal@legis.wisconsin.gov) or at (608) 266-3561. If you requested a fiscal estimate on an earlier version of this draft and would like to obtain a fiscal estimate on the current version before it is introduced, you will need to request a revised fiscal estimate from our program assistants.

**Please call our program assistants at (608) 266-3561 if you have any questions regarding this email.**