



PRELIMINARY DRAFT - NOT READY FOR INTRODUCTION

INSERT

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

Regeri

- 1 AN ACT *to create* 100.71 of the statutes; **relating to:** deletion of consumer
2 personal data by controllers. *and providing a penalty*

Analysis by the Legislative Reference Bureau

This bill generally requires controllers of consumers' personal data to delete a consumer's personal data if the consumer requests deletion of that personal data.

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 allows a consumer to request that a controller delete personal data relating to the consumer, and the controller must delete the personal data if certain conditions apply, such as the following: 1) it is no longer necessary for the controller to process the consumer's personal data to accomplish the purposes for which the personal data was collected or processed; or 2) the personal data is processed for direct marketing purposes. Under the bill, if a controller is required to delete a consumer's personal data and has disclosed the personal data, the controller must take reasonable steps based on the available technology and implementation cost to notify other controllers that are processing the personal data to delete the personal data, and other controllers so notified must also delete the personal data.

Various exceptions are provided under the bill, and under certain conditions, a controller is not required to delete personal data, such as if processing the personal data is necessary for performing a contract with the consumer, exercising the right

of free expression and information, complying with a legal obligation, or performing certain tasks carried out in the public interest.

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

134.985

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

100.71 Deleting consumer personal data. (1) DEFINITIONS. In this section:

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

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

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

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

(2) DELETING CONSUMER PERSONAL DATA. (a) 1. Except as provided in par. (b), upon a consumer's request, a controller shall delete without undue delay the personal data relating to the consumer if any of the following applies:

a. It is no longer necessary for the controller to process the personal data to accomplish the purposes for which the data was collected or processed.

b. The personal data is processed for direct marketing purposes.

INSA
Insert
crime tag

1 c. The personal data has been unlawfully processed.

2 d. Deleting the personal data is necessary to comply with a legal obligation to
3 which the controller is subject.

4 2. If a controller is required under this subsection to delete a consumer's
5 personal data and the controller has disclosed the personal data, the controller shall
6 take reasonable steps based on the available technology and implementation cost to
7 notify other controllers that are processing the consumer's personal data that the
8 consumer has requested that the controllers delete the consumer's personal data and
9 any links to the personal data. Except as provided in par. (b), upon receiving the
10 notice, the other controller shall delete the consumer's personal data.

11 3. a. Except as provided in subd. 3. b., if a controller is required under this
12 subsection to delete a consumer's personal data, the controller shall delete the
13 personal data and make any notification required under subd. 2. within one month
14 of receiving the consumer's request.

15 b. A controller may delete a consumer's personal data and make a notification
16 when required under this subsection within 3 months of receiving a consumer's
17 request if necessary due to the complexity and number of requests received by the
18 controller. If the controller does not delete the consumer's personal data and make
19 a notification under subd. 2. within one month of the consumer's request, the
20 controller shall within one month of the request inform the consumer about the delay
21 and notify the consumer of the reason for the delay.

INS 3-21 A

22 (b) A controller is not required to delete personal data under par. (a) if
23 processing the personal data is necessary for any of the following:

24 1. Performing a contract to which the consumer has agreed.

25 2. Exercising the right of free expression and information.

1 3. Complying with a legal obligation under federal, state, or local law.

2 4. Performing a task carried out in the public interest or in the exercise of
3 official authority vested in the controller.

4 5. Reasons of public interest in the area of public health, if the personal data
5 is processed by or under the responsibility of a professional subject to confidentiality
6 obligations under federal, state, or local law and any of the following applies:

7 a. Processing the personal data is necessary for purposes of preventive or
8 occupational medicine, for assessing the working capacity of an employee, for
9 medical diagnosis, or for providing health care or treatment.

10 b. Processing the personal data is necessary to protect against serious threats
11 to health or for ensuring the quality and safety of health care, medical products, or
12 medical devices.

13 6. Archiving purposes that are in the public interest, scientific or historical
14 research purposes, or statistical purposes, if deleting the personal data is likely to
15 render impossible or seriously impair achieving the objectives of the processing.

16 7. Establishing, exercising, or defending a legal claim.

17 (c) 1. This subsection does not require a controller to delete the following types
18 of information:

19 a. Health information protected by the federal Health Insurance Portability
20 and Accountability Act of 1996.

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

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

24 d. Information and documents created specifically for and collected and
25 maintained by a hospital.

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

3 f. Patient safety work product information for purposes of 42 USC 299b-21 to
4 299b-26.

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

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

11 i. Personal information collected, processed, sold, or disclosed pursuant to the
12 federal Gramm-Leach-Bliley Act, P.L. 106-102.

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

15 k. Information maintained for employment records.

16 2. This subsection does not require a consumer processing personal data in
17 connection with a purely personal or household activity to delete personal data.

INS 5-17 A

that
^

18 **SECTION 2. Effective date.**

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

20 (END)

**2019-2020 DRAFTING INSERT
FROM THE
LEGISLATIVE REFERENCE BUREAU**

LRB-4121/P3ins
KP:...

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 deletion requirements is subject to a fine of up to \$20,000,000 or of up to 4 percent of the controller's total annual revenue, whichever is greater.

2

3 END INS A

4 INS 3-21

5 4. A controller is not required to delete personal data under this paragraph if
6 the controller is unable to verify, using commercially reasonable efforts, the identity
7 of the consumer making the request.

8 END INS 3-21

9 INS 5-17

10 3. This subsection does not require a controller that obtains a consumer's
11 personal data for literary or artistic purposes to delete that personal data.

12 4. This subsection does not require a controller that obtains a consumer's
13 personal data, that intends to publish the personal data, and that believes that
14 publication of the personal data is in the public interest to delete that personal data.

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

18 **(4) ENFORCEMENT; PENALTY.** (a) The attorney general may investigate violations
19 of this section and may bring actions for enforcement of this section.

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

4 END INS 10-2

Paczuski, Konrad

From: Augustyn, Ryan <Ryan.Augustyn@legis.wisconsin.gov>

Sent: Thursday, September 26, 2019 4:13 PM

To: Paczuski, Konrad <Konrad.Paczuski@legis.wisconsin.gov>

Subject: Data Drafts

Hi Konrad,

Rep. Zimmerman has a few changes and would like to come back with p4 drafts on the bills.

- 1) Include in deletion bill that a company may refuse to delete if using data to stop a security incident.
- 2) For the penalties under the bills '10 mil or 2%, whichever is greater', remove the words 'whichever is greater' in all three drafts.

He also had a question of how the penalties would apply (would the fine be for each incident, or for a raft of incidents?).

Thank you,

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



State of Wisconsin
2019 - 2020 LEGISLATURE

LRB-4121/P3 *def*
KP:amn

PRELIMINARY DRAFT - NOT READY FOR INTRODUCTION

INSERT

IN: 10/1/2019
OUT: 10/2/2019

- 1 AN ACT *to create* 134.985 of the statutes; **relating to:** deletion of consumer
2 personal data by controllers and providing a penalty.

Analysis by the Legislative Reference Bureau

This bill generally requires controllers of consumers' personal data to delete a consumer's personal data if the consumer requests deletion of that personal data.

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 allows a consumer to request that a controller delete personal data relating to the consumer, and the controller must delete the personal data if certain conditions apply, such as the following: 1) it is no longer necessary for the controller to process the consumer's personal data to accomplish the purposes for which the personal data was collected or processed; or 2) the personal data is processed for direct marketing purposes. Under the bill, if a controller is required to delete a consumer's personal data and has disclosed the personal data, the controller must take reasonable steps based on the available technology and implementation cost to notify other controllers that are processing the personal data to delete the personal data, and other controllers so notified must also delete the personal data.

Various exceptions are provided under the bill, and under certain conditions, a controller is not required to delete personal data, such as if processing the personal data is necessary for performing a contract with the consumer, exercising the right of free expression and information, complying with a legal obligation, or performing certain tasks carried out in the public interest.

*shipping a
security
incident,*

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 deletion requirements is subject to a fine of up to \$20,000,000 or of up to 4 percent of the controller's total annual revenue, whichever is greater.

Because this bill creates a new crime or revises a penalty for an existing crime, the Joint Review Committee on Criminal Penalties may be requested to prepare a report.

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 Deleting consumer personal data. (1) DEFINITIONS.** In this
3 section:

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

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

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

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

1 **(2) DELETING CONSUMER PERSONAL DATA.** (a) 1. Except as provided in par. (b),
2 upon a consumer's request, a controller shall delete without undue delay the
3 personal data relating to the consumer if any of the following applies:

4 a. It is no longer necessary for the controller to process the personal data to
5 accomplish the purposes for which the data was collected or processed.

6 b. The personal data is processed for direct marketing purposes.

7 c. The personal data has been unlawfully processed.

8 d. Deleting the personal data is necessary to comply with a legal obligation to
9 which the controller is subject.

10 2. If a controller is required under this subsection to delete a consumer's
11 personal data and the controller has disclosed the personal data, the controller shall
12 take reasonable steps based on the available technology and implementation cost to
13 notify other controllers that are processing the consumer's personal data that the
14 consumer has requested that the controllers delete the consumer's personal data and
15 any links to the personal data. Except as provided in par. (b), upon receiving the
16 notice, the other controller shall delete the consumer's personal data.

17 3. a. Except as provided in subd. 3. b., if a controller is required under this
18 subsection to delete a consumer's personal data, the controller shall delete the
19 personal data and make any notification required under subd. 2. within one month
20 of receiving the consumer's request.

21 b. A controller may delete a consumer's personal data and make a notification
22 when required under this subsection within 3 months of receiving a consumer's
23 request if necessary due to the complexity and number of requests received by the
24 controller. If the controller does not delete the consumer's personal data and make
25 a notification under subd. 2. within one month of the consumer's request, the

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

3 4. A controller is not required to delete personal data under this paragraph if
4 the controller is unable to verify, using commercially reasonable efforts, the identity
5 of the consumer making the request.

6 (b) A controller is not required to delete personal data under par. (a) if
7 processing the personal data is necessary for any of the following:

8 1. Performing a contract to which the consumer has agreed.

9 2. Exercising the right of free expression and information.

10 3. Complying with a legal obligation under federal, state, or local law.

11 4. Performing a task carried out in the public interest or in the exercise of
12 official authority vested in the controller.

13 5. Reasons of public interest in the area of public health, if the personal data
14 is processed by or under the responsibility of a professional subject to confidentiality
15 obligations under federal, state, or local law and any of the following applies:

16 a. Processing the personal data is necessary for purposes of preventive or
17 occupational medicine, for assessing the working capacity of an employee, for
18 medical diagnosis, or for providing health care or treatment.

19 b. Processing the personal data is necessary to protect against serious threats
20 to health or for ensuring the quality and safety of health care, medical products, or
21 medical devices.

22 6. Archiving purposes that are in the public interest, scientific or historical
23 research purposes, or statistical purposes, if deleting the personal data is likely to
24 render impossible or seriously impair achieving the objectives of the processing.

25 7. Establishing, exercising, or defending a legal claim.

1 (c) 1. This subsection does not require a controller to delete the following types
2 of information:

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

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

6 c. 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 d. Information and documents created specifically for and collected and
9 maintained by a hospital.

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

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

14 g. 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 h. 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 i. Personal information collected, processed, sold, or disclosed pursuant to the
21 federal Gramm-Leach-Bliley Act, P.L. 106-102.

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

24 k. Information maintained for employment records.

**2019-2020 DRAFTING INSERT
FROM THE
LEGISLATIVE REFERENCE BUREAU**

LRB-4121/P4ins
KP:...

1 INS 4-8

2 2. Stopping a security incident.

3 END INS 4-8

4 INS 6-15

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

8 END INS 6-15

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



State of Wisconsin
2019 - 2020 LEGISLATURE

LRB-4121/P4 *De PS*
KP:amn

PRELIMINARY DRAFT - NOT READY FOR INTRODUCTION

INSERT

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

- 1 **AN ACT to create** 134.985 of the statutes; **relating to:** deletion of consumer
- 2 personal data by controllers and providing a penalty.

Analysis by the Legislative Reference Bureau

This bill generally requires controllers of consumers' personal data to delete a consumer's personal data if the consumer requests deletion of that personal data.

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 allows a consumer to request that a controller delete personal data relating to the consumer, and the controller must delete the personal data if certain conditions apply, such as the following: 1) it is no longer necessary for the controller to process the consumer's personal data to accomplish the purposes for which the personal data was collected or processed; or 2) the personal data is processed for direct marketing purposes. Under the bill, if a controller is required to delete a consumer's personal data and has disclosed the personal data, the controller must take reasonable steps based on the available technology and implementation cost to notify other controllers that are processing the personal data to delete the personal data, and other controllers so notified must also delete the personal data.

Various exceptions are provided under the bill, and under certain conditions, a controller is not required to delete personal data, such as if processing the personal data is necessary for performing a contract with the consumer, stopping a security incident, exercising the right of free expression and information, complying with a legal obligation, or performing certain tasks carried out in the public interest.

1) or if the personal data is processed by a political, philosophical, or religious nonprofit organization that processes only personal data of members, former members, or persons who have regular contact with the organization

other than information lawfully made available from federal, state, or local government records

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 deletion requirements is subject to a fine of up to \$20,000,000 or of up to 4 percent of the controller's total annual revenue, whichever is greater.

Because this bill creates a new crime or revises a penalty for an existing crime, the Joint Review Committee on Criminal Penalties may be requested to prepare a report.

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 Deleting consumer personal data. (1) DEFINITIONS.** In this
3 section:

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

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

8 (c) "Personal data" means information relating to a consumer that allows the
9 consumer to be identified, either directly or indirectly, including by reference to an
10 identifier such as a name, an identification number, location data, an online

11 identifier, or one or more factors related to the physical, physiological, genetic,^{yes}
12 mental, economic, cultural, or social identity of the consumer. *but does not include any information lawfully made available from federal, state, and local government records*

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

1 (2) DELETING CONSUMER PERSONAL DATA. (a) 1. Except as provided in par. (b),
2 upon a consumer's request, a controller shall delete without undue delay the
3 personal data relating to the consumer if any of the following applies:

4 a. It is no longer necessary for the controller to process the personal data to
5 accomplish the purposes for which the data was collected or processed.

6 b. The personal data is processed for direct marketing purposes.

7 c. The personal data has been unlawfully processed.

8 d. Deleting the personal data is necessary to comply with a legal obligation to
9 which the controller is subject.

10 2. If a controller is required under this subsection to delete a consumer's
11 personal data and the controller has disclosed the personal data, the controller shall
12 take reasonable steps based on the available technology and implementation cost to
13 notify other controllers that are processing the consumer's personal data that the
14 consumer has requested that the controllers delete the consumer's personal data and
15 any links to the personal data. Except as provided in par. (b), upon receiving the
16 notice, the other controller shall delete the consumer's personal data.

17 3. a. Except as provided in subd. 3. b., if a controller is required under this
18 subsection to delete a consumer's personal data, the controller shall delete the
19 personal data and make any notification required under subd. 2. within one month
20 of receiving the consumer's request.

21 b. A controller may delete a consumer's personal data and make a notification
22 when required under this subsection within 3 months of receiving a consumer's
23 request if necessary due to the complexity and number of requests received by the
24 controller. If the controller does not delete the consumer's personal data and make
25 a notification under subd. 2. within one month of the consumer's request, the

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

3 4. A controller is not required to delete personal data under this paragraph if
4 the controller is unable to verify, using commercially reasonable efforts, the identity
5 of the consumer making the request.

6 (b) A controller is not required to delete personal data under par. (a) if
7 processing the personal data is necessary for any of the following:

8 1. Performing a contract to which the consumer has agreed.

9 2. Stopping a security incident.

10 3. Exercising the right of free expression and information.

11 4. Complying with a legal obligation under federal, state, or local law.

12 5. Performing a task carried out in the public interest or in the exercise of
13 official authority vested in the controller.

14 6. Reasons of public interest in the area of public health, if the personal data
15 is processed by or under the responsibility of a professional subject to confidentiality
16 obligations under federal, state, or local law and any of the following applies:

17 a. Processing the personal data is necessary for purposes of preventive or
18 occupational medicine, for assessing the working capacity of an employee, for
19 medical diagnosis, or for providing health care or treatment.

20 b. Processing the personal data is necessary to protect against serious threats
21 to health or for ensuring the quality and safety of health care, medical products, or
22 medical devices.

23 7. Archiving purposes that are in the public interest, scientific or historical
24 research purposes, or statistical purposes, if deleting the personal data is likely to
25 render impossible or seriously impair achieving the objectives of the processing.

1 8. Establishing, exercising, or defending a legal claim.

2 (c) 1. This subsection does not require a controller to delete the following types
3 of information:

4 a. Health information protected by the federal Health Insurance Portability
5 and Accountability Act of 1996.

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

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

9 d. Information and documents created specifically for and collected and
10 maintained by a hospital.

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

13 f. Patient safety work product information for purposes of 42 USC 299b-21 to
14 299b-26.

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

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

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

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

25 k. Information maintained for employment records.

2019-2020 DRAFTING INSERT
FROM THE
LEGISLATIVE REFERENCE BUREAU

LRB-4121/P5ins
KP:...

1 INS 6-7

2 5. This subsection does not require a nonprofit organization having a political,
3 philosophical, or religious purpose that processes a consumer's personal data to
4 delete that personal data if all of the following applies: *apply*

5 a. The processing relates only to members or former members of the
6 organization or to persons who have regular contact with the organization related
7 the organization's purposes.

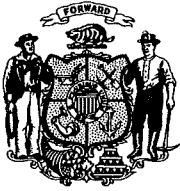
8 b. The personal data processed is not disclosed outside the organization.

9 END INS 6-7



Additional instructions from Rep. Zimmerman's office:

- Include an explicit exemption from the draft for law enforcement agencies
- Include in the draft a provision that specifically exempts personal data necessary for protecting against malicious, deceptive, fraudulent, or illegal activity or for prosecuting a person responsible for that activity from the deletion requirement.



PRELIMINARY DRAFT - NOT READY FOR INTRODUCTION

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

SAV
Pwf

Regen.

- 1 **AN ACT to create** 134.985 of the statutes; **relating to:** deletion of consumer
- 2 personal data by controllers and providing a penalty.

Analysis by the Legislative Reference Bureau

This bill generally requires controllers of consumers' personal data to delete a consumer's personal data if the consumer requests deletion of that personal data.

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 allows a consumer to request that a controller delete personal data relating to the consumer, and the controller must delete the personal data if certain conditions apply, such as the following: 1) it is no longer necessary for the controller to process the consumer's personal data to accomplish the purposes for which the personal data was collected or processed; or 2) the personal data is processed for direct marketing purposes. Under the bill, if a controller is required to delete a consumer's personal data and has disclosed the personal data, the controller must take reasonable steps based on the available technology and implementation cost to notify other controllers that are processing the personal data to delete the personal data, and other controllers so notified must also delete the personal data.

Various exceptions are provided under the bill, and under certain conditions, a controller is not required to delete personal data, such as if processing the personal data is necessary for performing a contract with the consumer, stopping a security

detecting or

protecting against malicious, deceptive, fraudulent, or illegal activity or prosecuting a person responsible for that activity,

incident, exercising the right of free expression and information, complying with a legal obligation, or performing certain tasks carried out in the public interest, or if the personal data is processed by a political, philosophical, or religious nonprofit organization that processes only personal data of members, former members, or persons who have regular contact with the organization.

Also, under the bill, the attorney general may investigate violations and bring actions for enforcement. A controller who violates the bill's personal data deletion requirements is subject to a fine of up to \$20,000,000 or of up to 4 percent of the controller's total annual revenue, whichever is greater.

Because this bill creates a new crime or revises a penalty for an existing crime, the Joint Review Committee on Criminal Penalties may be requested to prepare a report.

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 Deleting consumer personal data. (1) DEFINITIONS.** In this
3 section:

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

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

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

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

5 (2) DELETING CONSUMER PERSONAL DATA. (a) 1. Except as provided in par. (b),
6 upon a consumer's request, a controller shall delete without undue delay the
7 personal data relating to the consumer if any of the following applies:

8 a. It is no longer necessary for the controller to process the personal data to
9 accomplish the purposes for which the data was collected or processed.

10 b. The personal data is processed for direct marketing purposes.

11 c. The personal data has been unlawfully processed.

12 d. Deleting the personal data is necessary to comply with a legal obligation to
13 which the controller is subject.

14 2. If a controller is required under this subsection to delete a consumer's
15 personal data and the controller has disclosed the personal data, the controller shall
16 take reasonable steps based on the available technology and implementation cost to
17 notify other controllers that are processing the consumer's personal data that the
18 consumer has requested that the controllers delete the consumer's personal data and
19 any links to the personal data. Except as provided in par. (b), upon receiving the
20 notice, the other controller shall delete the consumer's personal data.

21 3. a. Except as provided in subd. 3. b., if a controller is required under this
22 subsection to delete a consumer's personal data, the controller shall delete the
23 personal data and make any notification required under subd. 2. within one month
24 of receiving the consumer's request.

1 b. A controller may delete a consumer's personal data and make a notification
2 when required under this subsection within 3 months of receiving a consumer's
3 request if necessary due to the complexity and number of requests received by the
4 controller. If the controller does not delete the consumer's personal data and make
5 a notification under subd. 2. within one month of the consumer's request, the
6 controller shall within one month of the request inform the consumer about the delay
7 and notify the consumer of the reason for the delay.

8 4. A controller is not required to delete personal data under this paragraph if
9 the controller is unable to verify, using commercially reasonable efforts, the identity
10 of the consumer making the request.

11 (b) A controller is not required to delete personal data under par. (a) if
12 processing the personal data is necessary for any of the following:

- 13 1. Performing a contract to which the consumer has agreed.
14 2. *Detecting or stopping* ~~Stopping~~ a security incident. *; protecting against malicious, deceptive, fraudulent, or illegal*
15 3. Exercising the right of free expression and information. *activity; or prosecuting a person responsible for*
16 4. Complying with a legal obligation under federal, state, or local law.
17 5. Performing a task carried out in the public interest or in the exercise of
18 official authority vested in the controller.

19 6. Reasons of public interest in the area of public health, if the personal data
20 is processed by or under the responsibility of a professional subject to confidentiality
21 obligations under federal, state, or local law and any of the following applies:

22 a. Processing the personal data is necessary for purposes of preventive or
23 occupational medicine, for assessing the working capacity of an employee, for
24 medical diagnosis, or for providing health care or treatment.

1 b. Processing the personal data is necessary to protect against serious threats
2 to health or for ensuring the quality and safety of health care, medical products, or
3 medical devices.

4 7. Archiving purposes that are in the public interest, scientific or historical
5 research purposes, or statistical purposes, if deleting the personal data is likely to
6 render impossible or seriously impair achieving the objectives of the processing.

7 8. Establishing, exercising, or defending a legal claim.

8 (c) 1. This subsection does not require a controller to delete the following types
9 of information:

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

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

13 c. 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 d. Information and documents created specifically for and collected and
16 maintained by a hospital.

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

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

21 g. 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.

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

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

8 k. Information maintained for employment records.

9 2. This subsection does not require a consumer processing personal data in
10 connection with a purely personal or household activity to delete that personal data.

11 3. This subsection does not require a controller that processes a consumer's
12 personal data for literary or artistic purposes to delete that personal data.

13 4. This subsection does not require 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 to delete that personal data.

16 5. This subsection does not require a nonprofit organization having a political,
17 philosophical, or religious purpose that processes a consumer's personal data to
18 delete that personal data if all of the following apply:

19 a. The processing relates only to members or former members of the
20 organization or to persons who have regular contact with the organization related
21 the organization's purposes.

22 b. The personal data processed is not disclosed outside the organization.

23 **(3) ENFORCEMENT; PENALTY.** (a) The attorney general may investigate violations
24 of this section and may bring actions for enforcement of this section.

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-4121/P6

KP:amn

NO
Change

PRELIMINARY DRAFT - NOT READY FOR INTRODUCTION

- 1 **AN ACT** *to create* 134.985 of the statutes; **relating to:** deletion of consumer
2 personal data by controllers and providing a penalty.

Analysis by the Legislative Reference Bureau

This bill generally requires controllers of consumers' personal data to delete a consumer's personal data if the consumer requests deletion of that personal data.

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 allows a consumer to request that a controller delete personal data relating to the consumer, and the controller must delete the personal data if certain conditions apply, such as the following: 1) it is no longer necessary for the controller to process the consumer's personal data to accomplish the purposes for which the personal data was collected or processed; or 2) the personal data is processed for direct marketing purposes. Under the bill, if a controller is required to delete a consumer's personal data and has disclosed the personal data, the controller must take reasonable steps based on the available technology and implementation cost to notify other controllers that are processing the personal data to delete the personal data, and other controllers so notified must also delete the personal data.

Various exceptions are provided under the bill, and under certain conditions, a controller is not required to delete personal data, such as if processing the personal data is necessary for performing a contract with the consumer, detecting or stopping

1 **(3) ENFORCEMENT, PENALTY.** (a) The attorney general may investigate violations
2 of this section and may bring actions for enforcement of this section.

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

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

9 **SECTION 2. Effective date.**

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

11

(END)

Walker, Dan

From: LRB.Legal
To: Rep.Zimmerman
Subject: Draft review: LRB -4121/1
Attachments: 19-4121/1

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, 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 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.