

2019 DRAFTING REQUEST**Bill**

For: **Shannon Zimmerman (608) 266-1526** Drafter: **kpaczusk**
 By: **Ryan** Secondary Drafters:
 Date: **8/27/2019** May Contact:

Same as LRB:

Submit via email: **YES**
 Requester's email: **Rep.Zimmerman@legis.wisconsin.gov**
 Carbon copy (CC) to: **konrad.paczuski@legis.wisconsin.gov**
mary.pfotenhauer@legis.wisconsin.gov

Pre Topic:

No specific pre topic given

Topic:

Consumer right to request controllers to delete personal data

Instructions:

See attached

Drafting History:

<u>Vers.</u>	<u>Drafted</u>	<u>Reviewed</u>	<u>Submitted</u>	<u>Jacketed</u>	<u>Required</u>
/?	kpaczusk 8/28/2019	anienaja 8/28/2019			
/P1	kpaczusk 9/5/2019	anienaja 9/6/2019	dwalker 8/28/2019		
/P2	kpaczusk 9/18/2019	anienaja 9/19/2019	dwalker 9/6/2019		
/P3	kpaczusk 10/1/2019	anienaja 10/2/2019	dwalker 9/19/2019		Crime
/P4	kpaczusk	anienaja	mbarman		Crime

<u>Vers.</u>	<u>Drafted</u>	<u>Reviewed</u>	<u>Submitted</u>	<u>Jacketed</u>	<u>Required</u>
/P5	kpaczusk 12/30/2019	anienaja 1/3/2020	dwalker 10/31/2019		Crime
/P6			mbarman 1/3/2020		Crime
/1			dwalker 1/23/2020	dwalker 1/23/2020	Crime

FE Sent For:

<END>

↳ Not
Needed



Meeting with Rep. Zimmermann's office 8/27:

Drafting instructions:

Draft a bill based on the provisions of the European Union's General Data Protection Regulation that require controllers of consumers' personal data to delete a consumer's personal data (mainly Article 17).

framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

- (10) 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
- (11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- (12) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- (13) 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
- (14) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
- (15) 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
- (16) 'main establishment' means:
 - (a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;
 - (b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;
- (17) 'representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;
- (18) 'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
- (19) 'group of undertakings' means a controlling undertaking and its controlled undertakings;
- (20) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;
- (21) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51;

- (22) 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because:
- (a) the controller or processor is established on the territory of the Member State of that supervisory authority;
 - (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
 - (c) a complaint has been lodged with that supervisory authority;
- (23) 'cross-border processing' means either:
- (a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
 - (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.
- (24) 'relevant and reasoned objection' means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;
- (25) 'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council ⁽¹⁾;
- (26) 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

CHAPTER II

Principles

Article 5

Principles relating to processing of personal data

1. Personal data shall be:
 - (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
 - (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
 - (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
 - (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

⁽¹⁾ Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.
3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

Article 9

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
2. Paragraph 1 shall not apply if one of the following applies:
 - (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
 - (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
 - (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
 - (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
 - (e) processing relates to personal data which are manifestly made public by the data subject;
 - (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
 - (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
 - (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
 - (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

*Article 15***Right of access by the data subject**

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- (a) the purposes of the processing;
- (b) the categories of personal data concerned;
- (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- (f) the right to lodge a complaint with a supervisory authority;
- (g) where the personal data are not collected from the data subject, any available information as to their source;
- (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

*Section 3***Rectification and erasure***Article 16***Right to rectification**

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

*Article 17***Right to erasure ('right to be forgotten')**

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

- (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- (d) the personal data have been unlawfully processed;
- (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

- (a) for exercising the right of freedom of expression and information;
- (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
- (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- (e) for the establishment, exercise or defence of legal claims.

Article 18

Right to restriction of processing

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

- (a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
- (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Article 19

Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Article 20

Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

- (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
- (b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Section 4

Right to object and automated individual decision-making

Article 21

Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

3. Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.

Article 86

Processing and public access to official documents

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

Article 87

Processing of the national identification number

Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

Article 88

Processing in the context of employment

1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 89

Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in

order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

Article 90

Obligations of secrecy

1. Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules shall apply only with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.

2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 91

Existing data protection rules of churches and religious associations

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing, such rules may continue to apply, provided that they are brought into line with this Regulation.

2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 of this Article shall be subject to the supervision of an independent supervisory authority, which may be specific, provided that it fulfils the conditions laid down in Chapter VI of this Regulation.

CHAPTER X

Delegated acts and implementing acts

Article 92

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.



PRELIMINARY DRAFT - NOT READY FOR INTRODUCTION

SA:
Xref:

IN: 8/28
OUT: 8/28

CPM:

1 AN ACT ...; **relating to:** requiring controllers to delete consumer personal
2 information ^{data}.

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) if 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; 2) if the controller has no legitimate ground to process the personal data that overrides the consumer's request; or 3) if 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 made that personal data public, the controller must take reasonable steps based on the available technology and implementation cost to inform other controllers that are processing the personal data to delete the personal data, and other controllers so notified must also delete the personal data.

disclosed the

notify

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 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:

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

2 **100.71 Deleting consumer 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.

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

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

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

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

20 b. The controller has no legitimate ground to process the personal data that
21 overrides the consumer’s request.

1 c. The personal data is processed for direct marketing purposes.

2 d. The personal data has been unlawfully processed.

3 e. Deleting the personal ^{data} is necessary to comply with a legal obligation to which
4 the controller is subject.

5 2. If a controller is required under subd. 1. to delete a consumer's personal data
6 and the controller has ^{e disclosed the personal data} ~~made the personal data public~~, the controller shall take

7 reasonable steps based on the available technology and implementation cost to

8 ^{e notify} ~~inform~~ other controllers that are processing the consumer's personal data that the

9 consumer has requested that the controllers delete the consumer's personal data and

10 any links to the personal data. Except as provided in par. (b), upon receiving the

11 ^{other} notice, the controller shall delete the consumer's personal data.

12 (b) Paragraph (a) does not require deleting personal data if processing the
13 personal data is necessary for any of the following:

14 1. Exercising the right of free expression and information.

15 2. Complying with a legal obligation under federal, state, or local law.

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

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

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

Paczuski, Konrad

From: Augustyn, Ryan <Ryan.Augustyn@legis.wisconsin.gov>
Sent: Tuesday, September 03, 2019 5:55 PM
To: Paczuski, Konrad <Konrad.Paczuski@legis.wisconsin.gov>
Subject: Data Notes

My notes cleaned up a bit:

Data notes:

1. See data (requiring controllers to provide access)
 - a. Include all exemptions from WA bill (3830) starting page 4, line 14
 - b. Requirement for companies to name controllers
 - c. Article 12 additions: Info shall be provided free of charge, except for requests manifestly unfounded or excessive (repetitive), the controller may either: (a) charge a reasonable fee for administrative costs or (b) refuse to act on the request (burden on the controller). Also does not apply if consumer has been provided information in the past.
 - d. Article 13: controller shall give contact information when data is collected.
 - e. Consumer should know what and whether decisions are made by automated processes or not
 - f. Article 14 provisions: data collected not from the consumer directly
 - g. In disclosure, tell the consumer they can request the halt of processing or deletion
 - h. Require notification of data breach

2. Stop Sale (restrict controllers from processing)
 - a. Does not define processor
 - b. Research: article 5(b): further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes
 - c. Article 6 processing exemptions: 1. Consent given, 2) necessary for a contract or to comply with consumer request prior to a contract, 3) to comply with legal obligations, 4. To protect another's rights, 5. To carry out business consumer expected providing data, except where children (12 and under) are involved (final point does not apply to public authorities).
 - d. Consent standard: be as easy to withdraw as to give consent. Controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data for specific uses of data
 - i. Article 4(11): Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. (plus article 7...be able to demonstrate consent was given for processing...clear and separate consent....able to withdraw anytime...
 - ii. you cannot require consent to data processing as a condition of using the service...except where necessary to perform service (Recital 42)
 - iii. recital 43, separate consent for each data processing operation (so email used for bettering the website vs. marketing must each get separate consent)
 - iv. Processing of 16 and under, consent must be given by a parent/guardian.
 - e. Add in article 9 prohibition on processing special categories with the list of exemptions

f. Article 30 requirements on processing activities

3. Request deletion

- a. Define 'no legitimate ground' to refer to exemptions starting on page 3, line 14; include to carry out a contract the consumer has agreed to?

Thoughts across the bills:

- Article 2: does not apply to: a natural person in purely personal or household activity
- Article 12(3): Controller complies with consumer requests within a month, which may be extended 2 further months where necessary, informing the subject either way.
- How would these bills treat facial recognition tech?
- Article 89 exceptions for research needed?

HAVE ADOPTED THIS REGULATION:

CHAPTER I

General provisions

Article 1

Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Article 2

Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
2. This Regulation does not apply to the processing of personal data:
 - (a) in the course of an activity which falls outside the scope of Union law;
 - (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;
 - (c) by a natural person in the course of a purely personal or household activity;
 - (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.
3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.
4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

Article 3

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

- (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.
4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Article 10

Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Article 11

Processing which does not require identification

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.
2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

CHAPTER III

Rights of the data subject

Section 1

Transparency and modalities

Article 12

Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

- (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
- (b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

Section 2

Information and access to personal data

Article 13

Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

- (a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
- (b) the contact details of the data protection officer, where applicable;
- (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;



State of Wisconsin
2019 - 2020 LEGISLATURE

LRB-4121/PT
KP:amn

PRELIMINARY DRAFT - NOT READY FOR INTRODUCTION

INSERT

IN: 9/5
OUT: 9/6

deletion of consumer personal data by controllers

- 1 AN ACT *to create* 100.71 of the statutes; **relating to:** requiring controllers to
2 delete consumer personal data.

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) if 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; 2) if the controller has no legitimate ground to process the personal data that overrides the consumer's request; or 3) if 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 exercising the right of free expression and information,

performing a contract with the consumer,

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:

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

2 **100.71 Deleting consumer 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.

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

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

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

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

20 b. The controller has no legitimate ground to process the personal data that
21 overrides the consumer's request.

- 1 ^{g.b.} (c) The personal data is processed for direct marketing purposes.
- 2 ^{ec.} (d) The personal data has been unlawfully processed.
- 3 ^{ed.} (e) Deleting the personal data is necessary to comply with a legal obligation to
- 4 which the controller is subject.

5 2. If a controller is required under ^{g this subsection} subd. 1. to delete a consumer's personal data

6 and the controller has disclosed the personal data, the controller shall take

7 reasonable steps based on the available technology and implementation cost to notify

8 other controllers that are processing the consumer's personal data that the consumer

9 has requested that the controllers delete the consumer's personal data and any links

10 to the personal data. Except as provided in par. (b), upon receiving the notice, the

11 other controller shall delete the consumer's personal data.

12 ^{INS 3-11} (b) Paragraph (a) does not require deleting personal data if processing the

13 personal data is necessary for any of the following:

14 ^{1. Performing a contract (that) the consumer has agreed to.} (1) Exercising the right of free expression and information.

15 ^{2.} (2) Complying with a legal obligation under federal, state, or local law.

16 ^{3.} (3) Performing a task carried out in the public interest or in the exercise of

17 official authority vested in the controller.

18 ^{4.} (4) Reasons of public interest in the area of public health, if the personal data

19 is processed by or under the responsibility of a professional subject to confidentiality

20 obligations under federal, state, or local law and any of the following applies:

21 a. Processing the personal data is necessary for purposes of preventive or

22 occupational medicine, for assessing the working capacity of an employee, for

23 medical diagnosis, or for providing health care or treatment.

2019-2020 DRAFTING INSERT
FROM THE
LEGISLATIVE REFERENCE BUREAU

LRB-4121/P2ins
KP:... *gmm*

1 INS 3-11

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

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

13 END INS 3-11

14 INS 4-7

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

17 a. Health information protected by the federal Health Insurance Portability
18 and Accountability Act of 1996.

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

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

22 d. Information and documents created specifically for and collected and
23 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.

18 END INS 4-7

Paczuski, Konrad

From: Augustyn, Ryan <Ryan.Augustyn@legis.wisconsin.gov>
Sent: Thursday, September 12, 2019 4:49 PM
To: Paczuski, Konrad <Konrad.Paczuski@legis.wisconsin.gov>
Subject: Updates to Privacy Bill Drafts

Hi Konrad,

We are nearing the end! Several changes he is looking for in the bills:

- The Attorney General will have the ability to investigate and enforce the law.
- Give consumers a private right of action, including banding together through third party groups.
- The penalties will be the same as GDPR. Change Euro amounts to dollar amounts (10 and 20 mil) but still keep it 2/4% global revenue cap. This link may help: <https://www.gdpreu.org/compliance/finest-and-penalties/>
- Remove the requirement to gain consent from processing for the following reasons: Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.
- Lastly, Shannon wanted me to double check that companies are able to verify when consumers make requests (so you can't spy on or delete someone else's data). I believe this is taken care of in the exceptions (i.e. if complying 'infringes on the rights of others'), but do we need to make this explicit?
 - o If we don't have this, we should add this provision: Where a controller has reasonable doubts concerning the identity of the consumer making a request under this section, the controller may request the provision of additional information necessary to confirm the identity of the consumer

Thank you as always for your work on this,

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

Paczuski, Konrad

From: Augustyn, Ryan <Ryan.Augustyn@legis.wisconsin.gov>
Sent: Wednesday, September 18, 2019 2:35 PM
To: Paczuski, Konrad <Konrad.Paczuski@legis.wisconsin.gov>
Subject: Data Bills

Hi Konrad,

Hope your week is going well.

Question for you, is journalism exempted from the bills as currently drafted? If not, then we should exempt journalism, as well as data used for literary and artistic purposes.

Not sure if you need this, but I saw one definition of journalism as holding personal data and believing 1) that you will publish the data and 2) that releasing the information to the public is in public interest. The medium also shouldn't matter (i.e. journalism in print, podcast, youtube, whatever should be exempt). The point is we don't want to stop journalism, publishing books, or the production of memes (maybe not high culture, but it would make me sad!)

Thank you,

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

6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

Article 83

General conditions for imposing administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.
2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:
 - (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
 - (b) the intentional or negligent character of the infringement;
 - (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
 - (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
 - (e) any relevant previous infringements by the controller or processor;
 - (f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
 - (g) the categories of personal data affected by the infringement;
 - (h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
 - (i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
 - (j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
 - (k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.
3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.
4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
 - (a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
 - (b) the obligations of the certification body pursuant to Articles 42 and 43;
 - (c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
- (b) the data subjects' rights pursuant to Articles 12 to 22;
- (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
- (d) any obligations pursuant to Member State law adopted under Chapter IX;
- (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

Article 84

Penalties

1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

CHAPTER IX

Provisions relating to specific processing situations

Article 85

Processing and freedom of expression and information

1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.