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 access personal data from controllers

Instructions:

See attached

Drafting History:

Vers.	Drafted	Reviewed	Submitted	Jacketed	Required
/?	kpaczusk 8/28/2019	aernsttr 8/28/2019			
/P1	kpaczusk 9/5/2019	aernsttr 9/6/2019	mbarman 8/28/2019		
/P2	kpaczusk 9/18/2019	anienaja 9/19/2019	lparisi 9/6/2019		
/P3	kpaczusk 10/2/2019	aernsttr 10/2/2019	mbarman 9/19/2019		
/P4	kpaczusk	aernsttr	jmurphy		

Vers.	Drafted	Reviewed	Submitted	Jacketed	Required
	10/30/2019	10/31/2019	10/2/2019		
/P5	kpaczusk 12/30/2019	aernsttr 1/2/2020	lparisi 10/31/2019		
/P6			mbarman 1/2/2020		
/1			dwalker 1/23/2020	dwalker 1/23/2020	

FE Sent For: **<END>**

→ Not Needed

Meeting with Rep. Zimmerman'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 personal data to provide consumers with a copy of their personal data (mainly Article 15).

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Article 4

Definitions

For the purposes of this Regulation:

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(3) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

(4) 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(5) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(6) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(9) 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the

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;

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;

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.

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Article 22

Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Section 5

Restrictions

Article 23

Restrictions

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

(a) national security;

(b) defence;

(c) public security;

State of Wisconsin
2019 - 2020 LEGISLATURE

LRB-4120/P1
KP:...
ahe

PRELIMINARY DRAFT - NOT READY FOR INTRODUCTION

IN: 8/28
OUT: 8/28

gen sav

AN ACT ...; **relating to:** requiring controllers to provide consumers with access to their personal data.

Analysis by the Legislative Reference Bureau

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

Under the bill, a "controller" is a person that alone or jointly with others determines the purposes and means of the processing of personal data. The bill defines "personal data" as information relating to a consumer that allows the consumer to be identified. The bill requires a controller, upon a consumer's request, to inform the consumer as to whether or not the controller processes the consumer's personal data.

Also, under the bill, if a controller processes a consumer's personal data, the controller must provide a copy of the personal data to a consumer who requests a copy. The controller must also provide the consumer with certain other information, including the purposes for which the controller processes the personal data, the categories of the personal data that the controller processes, and the persons to whom the controller discloses the personal data. If a consumer requests a copy of personal data electronically, the controller must provide the copy and requested information in a commonly used electronic form, unless the consumer requests otherwise. The bill allows a controller to charge a consumer a reasonable fee based on the administrative costs for providing copies of personal data other than the initial copy provided to the consumer. A controller is not required to provide a

consumer with a copy of the consumer's personal data if providing the copy would adversely affect the rights of others.

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

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

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

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

(b) "Controller" means a person that alone or jointly with others determines the purposes and means of the processing of personal data.

(c) "Personal data" means information relating to an consumer that allows the consumer to be identified, either directly or indirectly, including by reference to an identifier such as a name, 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 of 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.

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

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

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

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

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

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

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

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

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

3. The controller may charge the consumer a reasonable fee based on the administrative costs for providing copies of the personal data other than the initial copy provided to the consumer.

4. A controller is not required to provide a consumer with a copy under this paragraph if doing so would adversely affect the rights of others.

SECTION 2. Effective date.

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

(END)

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;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) 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.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Article 14

Information to be provided where personal data have not been obtained from the data subject

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with 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;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(e) the right to lodge a complaint with a supervisory authority;

(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

(g) 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.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 33

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Section 3

Data protection impact assessment and prior consultation

Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

State of Wisconsin
2019 - 2020 LEGISLATURE

LRB-4120/P1 ep2
KP:ahe

PRELIMINARY DRAFT - NOT READY FOR INTRODUCTION

INSERT

IN: 9/5
OUT: 9/6

consumer access to personal data processed by a controller

AN ACT ***to create*** 100.71 of the statutes; **relating to:** requiring controllers to provide consumers with access to their personal data.

Analysis by the Legislative Reference Bureau

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

Under the bill, a "controller" is a person that alone or jointly with others determines the purposes and means of the processing of personal data. The bill defines "personal data" as information relating to a consumer that allows the consumer to be identified. The bill requires a controller, upon a consumer's request, to inform the consumer as to whether or not the controller processes the consumer's personal data.

INS A

Also, under the bill, if a controller processes a consumer's personal data, the controller must provide a copy of the personal data to a consumer who requests a copy. The controller must also provide the consumer with certain other information, including the purposes for which the controller processes the personal data, the categories of the personal data that the controller processes, and the persons to whom the controller discloses the personal data. If a consumer requests a copy of personal data electronically, the controller must provide the copy and requested information in a commonly used electronic form, unless the consumer requests otherwise. The bill allows a controller to charge a consumer a reasonable fee based on the administrative costs for providing copies of personal data other than the initial copy provided to the consumer. A controller is not required to provide a

consumer with a copy of the consumer's personal data if providing the copy would adversely affect the rights of others.

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

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

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

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

(b) "Controller" means a person that alone or jointly with others determines the purposes and means of the processing of personal data.

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

(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.

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

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

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

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

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

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

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

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

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

INS 3-14 1

3. The controller may charge the consumer a reasonable fee based on the administrative costs for providing copies of the personal data other than the initial copy provided to the consumer.

4. A controller is not required to provide a consumer with a copy under this paragraph if doing so would adversely affect the rights of others.

SECTION 2. Effective date.

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

(END)

INS A

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

Under the bill, a "controller" is a person that alone or jointly with others determines the purposes and means of the processing of personal data. The bill defines "personal data" as information relating to a consumer that allows the consumer to be identified.

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

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

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

END INS A

INS 2-3

(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.

END INS 2-3

INS 2-10

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

END INS 2-10

INS 2-14

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

END INS 2-14

INS 2-15

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

1. The identity and contact information of the controller.

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

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

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

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

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

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

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

1. The identity and contact information of the controller.

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

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

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

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

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

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

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

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

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

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

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

END INS 2-15

INS 3-14

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

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

on the request. The controller bears the burden of demonstrating the a consumer's request is manifestly unfounded or excessive.

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

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

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

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

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

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

1. Reidentify data that does not identify a consumer.

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

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

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

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

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

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

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

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

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

(b) 1. Except as provided in subd. 2., if a controller is aware of a personal data breach of personal data maintained by the controller and the personal data breach

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

11. Information maintained for employment records.

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

END INS 3-14

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/fines-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?
    - 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.