

D R A F T  
FOR DISCUSSION ONLY

# Uniform Personal Data Protection Act

---

Uniform Law Commission

---

*June 4, 2021 Informal Session*



Copyright © 2021  
National Conference of Commissioners on Uniform State Laws

---

*This draft, including the proposed statutory language and any comments or reporter's notes, has not been reviewed or approved by the Uniform Law Commission or the drafting committee. It does not necessarily reflect the views of the Uniform Law Commission, its commissioners, the drafting committee, or the committee's members or reporter.*

May 27, 2021

## Uniform Personal Data Protection Act

The committee appointed by and representing the National Conference of Commissioners on Uniform State Laws in preparing this act consists of the following individuals:

Harvey S. Perlman	Nebraska, <i>Chair</i>
James Bopp Jr.	Indiana
Stephen Y. Chow	Massachusetts
Parrell D. Grossman	North Dakota
James C. McKay Jr.	District of Columbia
Larry Metz	Florida
James E. O'Connor	Nebraska
Robert J. Tennesen	Minnesota
Kerry Tipper	Colorado
Anthony C. Wisniewski	Maryland
Candace M. Zierdt	North Dakota
David V. Zvenyach	Wisconsin
William H. Henning	Alabama, <i>Division Chair</i>
Carl H. Lisman	Vermont, <i>President</i>

### Other Participants

Jane Bambauer	Arizona, <i>Reporter</i>
Michael Aisenberg	Virginia, <i>American Bar Association Advisor</i>
Daniel R. McGlynn	New Mexico, <i>American Bar Association Section Advisor</i>
Steven L. Willborn	Nebraska, <i>Style Liaison</i>
Tim Schnabel	Illinois, <i>Executive Director</i>

Copies of this act may be obtained from:

Uniform Law Commission  
111 N. Wabash Ave., Suite 1010  
Chicago, IL 60602  
(312) 450-6600  
[www.uniformlaws.org](http://www.uniformlaws.org)

# Uniform Personal Data Protection Act

## Table of Contents

Section 1. Title .....	1
Section 2. Definitions.....	1
Section 3. Scope.....	6
Section 4. Controller and Processor Responsibilities; General Provisions.....	8
Section 5. Right to Copy and Correct Personal Data.....	10
Section 6. Privacy Policy .....	13
Section 7. Compatible Data Practice .....	14
Section 8. Incompatible Data Practice .....	18
Section 9. Prohibited Data Practice .....	19
Section 10. Data Privacy and Security Risk Assessment .....	21
Section 11. Compliance with Other Law Protecting Personal Data .....	22
Section 12. Compliance with Voluntary Consensus Standard.....	24
Section 13. Content of Voluntary Consensus Standard .....	26
Section 14. Procedure for Development of Voluntary Consensus Standard .....	26
Section 15. Recognition of Voluntary Consensus Standard .....	27
Section 16. Applicability of [Consumer Protection Act].....	29
Section 17. Limits of Act.....	32
Section 18. Uniformity of Application and Construction.....	32
Section 19. Electronic Records and Signatures in Global and National Commerce Act .....	32
[Section 20. Severability].....	32
Section 21. Effective Date .....	32

1 **Uniform Personal Data Protection Act**

2 **Section 1. Title**

3 This [act] may be cited as the Uniform Personal Data Protection Act.

4 **Section 2. Definitions**

5 In this [act]:

6 (1) “Collecting controller” means a controller that collects personal data directly  
7 from a data subject.

8 (2) “Compatible data practice” means processing consistent with Section 7.

9 (3) “Controller” means a person that, alone or with others, determines the purpose  
10 and means of processing.

11 (4) “Data subject” means a resident of this state identified or described by  
12 personal data.

13 (5) “Deidentified data” means personal data that is modified to remove all direct  
14 identifiers and to reasonably ensure that the record cannot be linked to an identified data subject  
15 by a person that does not have personal knowledge or special access to the data subject’s  
16 information.

17 (6) “Direct identifier” means information that is commonly used to identify a data  
18 subject, including name, physical address, email address, recognizable photograph, telephone  
19 number, and Social Security number.

20 (7) “Incompatible data practice” means processing that may be performed  
21 lawfully under Section 8.

22 (8) “Maintains,” with respect to personal data, means to retain, hold, store, or  
23 preserve personal data as a system of records used to retrieve records about individual data

1 subjects for the purpose of individualized communication or decisional treatment.

2 (9) “Person” means an individual, estate, business or nonprofit entity, or other  
3 legal entity. The term does not include a public corporation or government or governmental  
4 subdivision, agency, or instrumentality.

5 (10) “Personal data” means a record that identifies or describes a data subject by a  
6 direct identifier or is pseudonymized data. The term does not include deidentified data.

7 (11) “Processing” means performing or directing performance of an operation on  
8 personal data, including collection, transmission, use, disclosure, analysis, prediction, and  
9 modification of the personal data, whether or not by automated means. “Process” has a  
10 corresponding meaning.

11 (12) “Processor” means a person that processes personal data on behalf of a  
12 controller.

13 (13) “Prohibited data practice” means processing prohibited by Section 9.

14 (14) “Pseudonymized data” means personal data without a direct identifier but  
15 that can be reasonably linked to a data subject’s identity or is maintained to allow individualized  
16 communication with, or treatment of, the data subject. The term does not include deidentified  
17 data. The term does include a record without a direct identifier but containing an internet  
18 protocol address, a browser, software, or hardware identification code, a persistent unique code  
19 that is not a direct identifier, or other data related to a particular device.

20 (15) “Publicly available information” means information:

21 (A) lawfully made available from a federal, state, or local government  
22 record;

23 (B) available to the general public in widely distributed media, including:

- 1 (i) a publicly accessible website;
- 2 (ii) a website or other forum with restricted access if the
- 3 information is available to a broad audience;
- 4 (iii) a telephone book or online directory;
- 5 (iv) a television, Internet, or radio program; and
- 6 (v) news media;
- 7 (C) observable from a publicly accessible location; or
- 8 (D) that an individual reasonably believes is lawfully made available to
- 9 the general public if:

10 (i) the information is of a type generally available to the public;

11 and

12 (ii) the individual has no reason to believe that a data subject with

13 authority to remove the information from public availability has directed the information to be

14 removed.

15 (16) "Record" means information:

- 16 (A) inscribed on a tangible medium; or
- 17 (B) stored in an electronic or other medium and retrievable in perceivable
- 18 form.

19 (17) "Sensitive data" means personal data that reveals:

- 20 (A) racial or ethnic origin, religious belief, gender, sexual orientation,
- 21 citizenship, or immigration status;
- 22 (B) credentials sufficient to access an account remotely;
- 23 (C) a credit or debit card number or financial account number;

1 (D) a Social Security number, tax-identification number, driver’s license  
2 number, military identification number, or an identifying number on a governmental-issued  
3 identification;

4 (E) geolocation in real time;

5 (F) a criminal record;

6 (G) diagnosis or treatment for a disease or health condition;

7 (H) genetic sequencing information; or

8 (I) information about a data subject the controller knows or has reason to  
9 know is under 13 years of age.

10 (18) “Sign” means, with present intent to authenticate or adopt a record:

11 (A) execute or adopt a tangible symbol; or

12 (B) attach to or logically associate with the record an electronic symbol,  
13 sound, or procedure.

14 (19) “Stakeholder” means a person that has, or represents a person that has, a  
15 direct interest in the development of a voluntary consensus standard.

16 (20) “State” means a state of the United States, the District of Columbia, Puerto  
17 Rico, the United States Virgin Islands, or any other territory or possession subject to the  
18 jurisdiction of the United States. The term includes a federally recognized Indian tribe.

19 (21) “Third-party controller” means a controller that receives from another  
20 controller authorized access to personal data or pseudonymized data and determines the purpose  
21 and means of additional processing.

22 **Comment**

23  
24 The Act regulates the processing of personal data. Throughout the Act uses the terms  
25 “information,” “record,” and “personal data” as increasingly specific categories. Information

1 would include all potentially interpretable signs and symbols, in any form, that create knowledge  
2 about any subject. A “record” is information that is recorded in an electronic or tangible medium.  
3 Records are a subset of information. “Personal data” is the subset of records that describe an  
4 individual. The Act avoids using the term “data” on its own, as this would be coterminous with  
5 “record.” References to “data” only appear in phrases such as “personal data” or “compatible  
6 data practice” that are defined terms in this Act.  
7

8 The Act recognizes the distinction between controllers and processors. A controller is the  
9 person who determines the purpose and means of data processing. There are two types of  
10 controllers. A “collecting controller” is a person who directly collects data from a data subject  
11 and thus has a relationship with the data subject. A “third party controller” is a person who  
12 obtains personal data not directly from data subjects but from another controller, generally a  
13 collecting controller. As long as the person directs the purpose and means of a data processing  
14 the person is a data controller. A processor, on the other hand, processes personal data at the  
15 direction of a controller; a processor does not determine the purpose of processing of personal  
16 data. However, if a person with access to personal data engages in processing that is not at the  
17 direction and request of a controller, that person becomes a controller rather than a processor,  
18 and is therefore subject to the obligations and constraints of a controller.  
19

20 The language in (3) that requires the controller to dictate both the “purpose and means”  
21 of processing is intended to include within the term “means” the selection of the processor to  
22 perform the processing.  
23

24 The definition of “maintains” is pivotal to understanding the scope of the act. It is  
25 modeled after the federal Privacy Act’s definitions of “maintains” and “system of records”. 5  
26 U.S.C. §552a(a)(3), (a)(5). While many individuals and businesses may accumulate data related  
27 to individuals in the form of emails or personal photographs, these records are not maintained as  
28 a system for the purpose and function of making individualized assessments, decisions, or  
29 communications, and would therefore not qualify under its scope in Section 3.  
30

31 Personal data and deidentified data are mutually exclusive categories. Deidentified data  
32 must meet the standard of risk mitigation that makes data reasonably unlikely to be reidentified.  
33 This reasonableness standard is flexible so that it can accommodate advances in technology or  
34 data availability that may make reidentification efforts easier over time. Thus, the standard can  
35 be expected to rise as the ability to reidentify anonymized datasets rises. However, this is not a  
36 strict liability standard, nor is it one intolerant to risk. If reidentification is costly and error-prone,  
37 the data can meet the standard for de-identification even if reidentification is possible.  
38

39 The broad category of “personal data” includes both direct identifying data and  
40 pseudonymized data. Data with a direct identifier (like name, social security number, or address)  
41 receives the full set of data protections under the act. By contrast, controllers using  
42 pseudonymized data are released from the requirement to provide access and correction (except  
43 in the case of sensitive pseudonymized data that is maintained in a way that renders the data  
44 retrievable for individualized communications and treatment.)  
45

46 The definition of a “direct identifier” is limited to information that on its own tends to



1 identify and relate specifically to an individual. The definition provides an illustrative list of  
2 examples, but the list is non-exhaustive so that the definition is flexible enough to cover new  
3 forms of identification that emerge in the future. A persistent unique code that is used to track or  
4 communicate with an individual without identifying them is *not* a direct identifier, even if that  
5 unique code can be converted into a direct identifier using a decryption key. Data that includes a  
6 persistent unique code (but not the decryption key) is pseudonymized data. Data that does not  
7 include direct identifiers or persistent unique IDs maintained for individualized communication  
8 and treatment will nevertheless be pseudonymized data (as opposed to deidentified data) if it  
9 presents a reasonable risk of reidentification.

10  
11 Pseudonymized data is itself a large subset of personal data that encompasses two distinct  
12 data practices, as identified by each of the clauses in the first sentence of its definition. First,  
13 some firms redact or remove direct identifiers and use the rest of the data fields for aggregate  
14 analysis or research. This usage of pseudonymized data is analogous to the intended uses of  
15 deidentified data, but the data does not qualify as deidentified because it is still “reasonably  
16 linkable to a data subject’s identity.” A second common practice is to maintain data without  
17 direct identifiers but with a unique code that permits firms to use the data for “individualized  
18 communication with, or treatment of, the data subject.” Cookie IDs, browser codes, and IP  
19 addresses have historically been used for this purpose. Both types of practices fall under the  
20 umbrella term “pseudonymized data” and are covered by many of the data protections of this act.  
21 However, pseudonymized data that is not maintained for individualized communication or  
22 treatment is not subject to the rights of access and correction. Pseudonymized data that is  
23 maintained for individualized communication or treatment is only subject to the rights of access  
24 and correction if the data includes sensitive data. Both types of pseudonymized data should have  
25 a more limited set of legal restrictions and obligations in order to incentivize the good data  
26 hygiene and practice of removing direct identifiers. *See Paul Schwartz & Daniel Solove, The PII*  
27 *Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 NYU L. REV.  
28 1814 (2011).

29  
30 The act exempts public records, lawfully obtained. Laws providing for the collection,  
31 retention, and use of public records may contain privacy and security requirements or limits on  
32 how the records may be accessed and used. This act does not interfere with those other  
33 provisions.

34  
35 The definition of “publicly available information” includes information accessible from a  
36 public website as well as information that is available on a nonpublic portion of a website if that  
37 nonpublic portion is nevertheless available to a large, non-intimate group of individuals. For  
38 example, if an individual shares personal data about themselves in a social media post that is  
39 accessible to all connected friends, that information is publicly available and would not fall  
40 within the scope of this Act. However, personal data that is shared with a hand-selected subset of  
41 friends through a direct message or through a highly constrained post on social media would not  
42 be publicly available.

### 43 44 **Section 3. Scope**

45 (a) This [act] applies to the activities of a controller or processor that conducts business in

1 this state or produces products or provides services purposefully directed to residents of this state  
2 and:

3 (1) maintains personal data about more than [50,000] data subjects during a  
4 calendar year;

5 (2) earns more than [50] percent of its gross annual revenue during a calendar  
6 year from maintaining personal data from data subjects as a controller or processor;

7 (3) is a processor acting on behalf of a controller the processor knows or has  
8 reason to know satisfies paragraph (1) or (2); or

9 (4) maintains personal data, unless it processes the personal data solely using  
10 compatible data practices.

11 (b) This [act] does not apply to an agency or instrumentality of this state or a political  
12 subdivision of this state.

13 (c) This [act] does not apply to personal data that is:

14 (1) publicly available information;

15 (2) processed solely as part of human-subjects research conducted in compliance  
16 with legal requirements for the protection of human subjects;

17 (3) disclosed as required or permitted by a warrant, subpoena, or court order or rule, or  
18 otherwise as specifically required by law;

19 (4) subject to a public-disclosure requirement under [cite to state public records  
20 act]; or

21 (5) processed in the course of a data subject's employment or application for  
22 employment.

23 **Comment**  
24

1 The definition of “personal data” limits that term to data describing residents of this state.  
2 This section further constrains the scope of the Act by limiting the controllers and processors  
3 obligated to comply with the act. Personal data privacy legislation can impose significant  
4 compliance costs on controllers and processors and thus most proposals contain limits similar to  
5 those in subsections (1), (2), and (3) which limit their provisions to larger controllers or  
6 processors—ones who either process data on a significant number of data subjects or earn a  
7 significant amount of their revenue from processing personal data. The threshold numbers are in  
8 brackets and each State can determine the proper level of applicability. The main goal of the act  
9 is to ensure data is secured and used in responsible ways, and the primary compliance  
10 mechanisms imposed are the obligation to publish a privacy policy and to conduct a privacy  
11 assessment in order to make their data practices transparent. Similarly, these firms must respond  
12 to consumer access and correction rights. The result of the limitations in (a) (1)-(3), however, is  
13 to put personal data at risk when collected by smaller firms. Thus, this act also applies to smaller  
14 firms, but relieves them of the compliance obligations as long as they use the personal data only  
15 for compatible purposes.

16  
17 By moving away from data subject consent as the basis for data processing and  
18 recognizing that data collectors are entitled to process data for compatible uses, some significant  
19 compliance costs are accordingly reduced, while placing limits on incompatible or unexpected  
20 and risky uses of data.

21  
22 The processing of publicly available information is excluded from the act. There are  
23 significant First Amendment implication for placing limits on the use of public information.  
24 “Publicly available information” is defined in Section 2 of this act.

25  
26 Processors and controllers who do not conduct business or market products and services  
27 to this state are outside the scope of the act.

#### 28 **Section 4. Controller and Processor Responsibilities; General Provisions**

29 (a) A controller shall:

30  
31 (1) if a collecting controller, provide under Section 5 a copy of a data subject’s  
32 personal data to the data subject on request;

33 (2) correct or amend a data subject’s personal data on the data subject’s request  
34 under Section 5;

35 (3) provide notice and transparency under Section 6 about the personal data it  
36 maintains and its processing practices;

37 (4) obtain consent for processing that, without consent, would be an incompatible

1 data practice under Section 8;  
2 (5) abstain from using a prohibited data practice;  
3 (6) conduct and maintain data privacy and security risk assessments under Section  
4 10; and  
5 (7) provide redress for an incompatible data practice or prohibited data practice  
6 the controller performs or is responsible for performing while processing a data subject's  
7 personal data.

8 (b) A processor shall:

9 (1) on request of the controller, provide the controller with a data subject's  
10 personal data or enable the controller to access the personal data at no cost to the controller;

11 (2) correct an inaccuracy in a data subject's personal data on request of the  
12 controller;

13 (3) abstain from processing personal data for a purpose other than one requested  
14 by the controller;

15 (4) conduct and maintain data privacy and security risk assessments in accordance  
16 with Section 10; and

17 (5) provide redress for an incompatible or prohibited data practice the processor  
18 knowingly performs in the course of processing a data subject's personal data at the direction of  
19 the controller.

20 (c) A controller or processor is responsible for an incompatible data practice or prohibited  
21 data practice committed by another if:

22 (1) the practice is committed with respect to personal data collected by the controller  
23 or processed by the processor; and

1 (2) the controller or processor knew the personal data would be used for the practice  
2 and was in a position to prevent it.

### 3 **Comment**

4  
5 This Part clarifies the different obligations that collecting controllers, third party  
6 controllers, and data processors owe to individuals. Third party controllers, including data  
7 brokers, are firms that decide how data is processed. They are under most of the same obligations  
8 as collecting controllers. However, they are not under the obligation to respond to access or  
9 correction requests. A right of access or correction imposed on third party controllers would  
10 increase privacy and security vulnerabilities because third party controllers are not able to verify  
11 the authenticity of the request as easily as collecting controllers. However, collecting controllers  
12 must transmit credible collection requests to downstream third party controllers and data  
13 processors who have access to the personal data requiring correction.  
14

15 Subsection (c) makes clear that a malfeasant in a supply chain that violates the act can  
16 expose their business partners to liability risk if those partners had sufficient information to know  
17 what the malfeasant was doing. This ensures that all actors have incentive to avoid working with  
18 irresponsible firms, to refuse to process data in a manner that is prohibited, and to end  
19 relationships with downstream processors or third party controllers that violate the act.  
20

21 This Act does not obligate controllers or processors to delete data at the request of the  
22 data subject. This is substantially different from the GDPR, the California Consumer Privacy  
23 Act, and several privacy bills recently introduced in state legislatures. There is a wide range of  
24 legitimate interests on the part of collectors that require data retention. It also appears difficult  
25 given how data is currently stored and processed to assure that any particular data subject's data  
26 is deleted. The restriction on processing for compatible uses or incompatible uses with consent  
27 should provide sufficient protection.  
28

### 29 **Section 5. Right to Copy and Correct Personal Data**

30 (a) Unless personal data is pseudonymized and not maintained with sensitive data, the  
31 collecting controller, with respect to personal data initially collected by the controller and  
32 maintained by the controller or a third-party controller or processor, shall:

33 (1) establish a reasonable procedure for a data subject to request, receive a copy  
34 of, and propose an amendment or correction to personal data about the data subject;

35 (2) establish a procedure to authenticate the identity of a data subject who  
36 requests a copy of the data subject's personal data;

1 (3) comply with a request from an authenticated data subject for a copy of  
2 personal data about the data subject [not later than 45 days] [within a reasonable time] after  
3 receiving it or provide an explanation of action being taken to comply with the request;

4 (4) on request, provide the data subject one copy of the data subject's personal  
5 data free of charge once every 12 months and additional copies on payment of a fee reasonably  
6 based on administrative costs;

7 (5) make an amendment or correction requested by a data subject if the controller  
8 has no reason to believe the request is unreasonable or excessive; and

9 (6) confirm to the data subject that an amendment or correction has been made or  
10 explain why the amendment or correction has not been made.

11 (b) A collecting controller shall make a reasonable effort to ensure that a correction of  
12 personal data performed by the controller also is performed on personal data maintained by a  
13 third-party controller or processor that directly or indirectly received personal data from the  
14 collecting controller. A third-party controller or processor shall make a reasonable effort to assist  
15 the collecting controller, if necessary to satisfy a request of a data subject under this section.

16 (c) A controller may not deny a good or service, charge a different rate, or provide a  
17 different level of quality to a data subject in retaliation for exercising a right under this section. It  
18 is not retaliation under this subsection for a controller to make a data subject ineligible to  
19 participate in a program if:

20 (1) the corrected information requested by the data subject makes the data subject  
21 ineligible for the program; and

22 (2) the program's terms of service specify the eligibility requirements for all  
23 participants.

1 (d) An agreement that waives or limits a right or duty under this section is contrary to  
2 public policy and unenforceable.

### 3 **Comment**

4  
5 The requirement to provide a copy of data or to initiate a data correction applies only to  
6 collecting controllers. These are the firms that already necessarily have a relationship with the  
7 data subject such that a secure authentication process would not unduly burden their business. A  
8 collecting controller must transmit any reasonable request for data correction to third party  
9 controllers and processors and make reasonable efforts to ensure that these third parties have  
10 actually made the requested change. Any third-party controller that receives a request for  
11 correction from a collecting controller must transmit the request to any processor or other third-  
12 party controller that it has engaged so that the entire chain of custody of personal data is  
13 corrected.

14  
15 A collecting controller that controls and maintains personal data from several sources,  
16 only some of which were originally collected by the collecting controller, must nevertheless  
17 provide access to and correction of all personal data that the collecting controller has associated  
18 with the data subject. Thus, if a collecting controller comingles personal data collected directly  
19 from the data subject with data that has been collected or accessed from other sources (including  
20 public sources and from other firms who share federated data) but is linked data subject, the  
21 access and correction rights apply to the entire set of personal data.

22  
23 Access and correction rights do not apply to pseudonymized data in most cases. The only  
24 time a collecting controller will have to provide access and correction to pseudonymized data is  
25 if the data contains sensitive data, *and* the collecting controller maintains the data so that it can  
26 and will be re-associated with an individual at a later date (or transmits the pseudonymized data  
27 to a third party for its use in this way.) A collecting controller that stores user credentials and  
28 profiles of its customers can avoid the access and correction obligations if it segregates its data  
29 into a key code and a pseudonymized database so that the data fields are stored with a unique  
30 code and no identifiers. The separate key will allow the controller to reidentify a user's data  
31 when necessary or relevant for their interactions with the customers. Likewise, a collecting  
32 controller that creates a dataset for its own research use (without maintaining it in a way that  
33 allows for reassociation with the data subject) will not have to provide access or correction rights  
34 even if the pseudonymized data includes sensitive information such as gender or race. A retailer  
35 that collects and transmits credit card data to the issuer of the credit card in order to facilitate a  
36 one-time credit card transactions is not maintaining this sensitive pseudonymized data.

37  
38 Subpart (c) ensures that a data subject who uses a right to access or correction is not  
39 penalized through diminished services or access for using their rights. This anti-discrimination  
40 provision is narrower than those appearing in statutes that also provide a right to deletion. A  
41 variety of firms follow a business model that provides their services for free or at a reduced rate  
42 in exchange for their customers providing personal data. This provision does not affect such a  
43 business model. For a denial to be prohibited by this section it must be in retaliation for a data  
44 subject's exercise of a right to access or correct data. Not every change in service following a

1 correction of data is discriminatory. For example, a loyalty or membership club that requires  
2 members to live in a certain region may make a member ineligible for benefits if the correction  
3 to the data shows an address outside the region. Similarly, a correction of data that shows a  
4 significant increase in the data subject's risk profile may justify an increase in insurance  
5 premium rates. Neither of these or similar actions would be "retaliation" under this section.  
6

## 7 **Section 6. Privacy Policy**

8 (a) A controller shall adopt and comply with a reasonably clear and accessible privacy  
9 policy that discloses:

10 (1) categories of personal data maintained by or on behalf of the controller;

11 (2) categories of personal data the controller provides to a processor or another  
12 controller and the purpose of providing the personal data;

13 (3) compatible data practices applied routinely to personal data by the controller  
14 or by an authorized processor;

15 (4) incompatible data practices that, unless the data subject withholds consent,  
16 will be applied by the controller or an authorized processor to personal data;

17 (5) the procedure for a data subject to exercise a right under Section 5;

18 (6) federal, state, or international privacy laws or frameworks with which the  
19 controller complies; and

20 (7) any voluntary consensus standard adopted by the controller.

21 (b) The privacy policy under subsection (a) must be reasonably available to a data subject  
22 at the time personal data is collected about the subject.

23 (c) If a controller maintains a public website, the controller shall publish the privacy  
24 policy on the website.

25 (d) The [Attorney General] may review the privacy policy of a controller for compliance  
26 with this section.



1 **Comment**

2  
3 The purpose of the required privacy policy is to provide data subjects with a transparent  
4 way to determine the scope of the data processing conducted by collecting controllers. While  
5 consent to compatible data practices is not required, the privacy policy does assure that data  
6 subjects can understand what those practices are for a particular controller and may choose not to  
7 engage with that controller or its affiliates. Thus, this helps to promote an autonomy regime for  
8 individuals with high levels of privacy concern without requiring burdensome consent  
9 instruments. The privacy policy also permits consumer advocates and the Attorney General to  
10 monitor data practices and to take appropriate action.

11  
12 Controllers and processors must describe all of the personal data routinely maintained  
13 about data subjects including pseudonymized data. They must also describe compatible data  
14 practices and incompatible data practices employed with consent under Section 8 that are  
15 currently in routine use. Because the privacy policy requirement applies only to “maintained”  
16 data, controllers do not have to provide disclosures related to personal data (whether directly  
17 identified or pseudonymized) that are not used as a system of records for individualized  
18 communications or treatment. For example, email systems or pseudonymized statistical data  
19 typically would not be subject to this privacy policy requirement.

20  
21 Controllers and processors do not have to explicitly state compatible data practices that  
22 are not routinely used. For example, a controller may disclose personal data that provides  
23 evidence of criminal activity to a law enforcement agency without listing this practice in its  
24 privacy policy as long as this type of disclosure is unusual.

25  
26 Subsection (b) requires the privacy policy to be reasonably available to the data subject at  
27 the time data is collected. This does not require providing a data subject with individual notice.  
28 Placement of the privacy policy on a public website or posting in a location that is accessible to  
29 data subjects is sufficient.

30  
31 The act does not require a controller to adopt and comply with a single or comprehensive  
32 set of voluntary consensus standards. However, if the controller does adopt such a standard, that  
33 should be stated in the privacy policy.

34  
35 **Section 7. Compatible Data Practice**

36 (a) A controller or processor may engage in a compatible data practice without the data  
37 subject’s consent. A controller or processor engages in a compatible data practice if the processing is  
38 consistent with the ordinary expectations of data subjects or is likely to benefit data subject  
39 substantially. The following factors apply to determine whether processing is a compatible data  
40 practice:

- 1 (1) the data subject’s relationship with the controller;
  - 2 (2) the type of transaction in which the personal data was collected;
  - 3 (3) the type and nature of the personal data that would be processed;
  - 4 (4) the risk of a negative consequence on the data subject by the use or disclosure of
  - 5 the personal data;
  - 6 (5) the effectiveness of a safeguard against unauthorized use or disclosure of the
  - 7 personal data; and
  - 8 (6) the extent to which the practice advances the economic, health, or other
  - 9 interests of the data subject.
- 10 (b) A compatible data practice includes processing that:
- 11 (1) initiates or effectuates a transaction with a data subject with the subject’s
  - 12 knowledge or participation;
  - 13 (2) is reasonably necessary to comply with a legal obligation or regulatory oversight
  - 14 of the controller;
  - 15 (3) meets a particular and explainable managerial, personnel, administrative, or
  - 16 operational need of the controller or processor;
  - 17 (4) permits appropriate internal oversight of the controller or external oversight by a
  - 18 government unit or the controller’s or processor’s agent;
  - 19 (5) is reasonably necessary to create pseudonymized or deidentified data;
  - 20 (6) permits analysis for generalized research or research and development of a new
  - 21 product or service;
  - 22 (7) is reasonably necessary to prevent, detect, investigate, report on, prosecute, or
  - 23 remediate an actual or potential:

- 1 (A) fraud;
- 2 (B) unauthorized transaction or claim;
- 3 (C) security incident;
- 4 (D) malicious, deceptive, or illegal activity;
- 5 (E) legal liability of the controller; or
- 6 (F) threat to national security;
- 7 (8) assists a person or government entity acting under paragraph (7);
- 8 (9) is reasonably necessary to comply with or defend a legal claim; or
- 9 (10) any other purpose determined to be a compatible data practice under
- 10 subsection (a).

11 (c) A controller may use personal data, or disclose pseudonymized data to a third-party  
12 controller, to deliver targeted advertising and other purely expressive content to a data subject.  
13 Under this subsection a controller may not use personal data or disclose pseudonymized data to  
14 be used to offer terms, including terms relating to price or quality, to a data subject that are  
15 different from terms offered to data subjects generally. Processing personal data or  
16 pseudonymized data for differential treatment is an incompatible data practice unless the  
17 processing is otherwise compatible under this section. This subsection does not prevent  
18 providing special considerations to members of a program if the program’s terms of service  
19 specify the eligibility requirements for all participants.

20 (d) A controller or processor may process personal data in accordance with the rules of a  
21 voluntary consensus standard under Sections 12 through 14 unless a court has prohibited the  
22 processing or found it to be an incompatible data practice. To permit processing under a  
23 voluntary consensus standard, a controller must commit to the standard in its privacy policy.

1 **Comment**

2  
3 Compatible data practices are mutually exclusive from incompatible and prohibited data  
4 practices described in Sections 8 and 9. Although compatible practices do not require specific  
5 consent from each data subject, they nevertheless must be reflected in the publicly available privacy  
6 policy as required by Section 6.  
7

8 Subsection (a) provides a list of factors that can help determine whether a practice is or is not  
9 compatible. Subsection (b) provides a list of nine specific practices that are per se compatible and do  
10 not require consent from the data subject followed by a tenth gap-filling category that covers any  
11 other processing that meets the more abstract definition of “compatible data practice.” The factors  
12 listed in subsection (a) inform how the scope of “compatible data practice” should be interpreted. The  
13 catch-all provision in (b)(10) allows controllers and processors to create innovative data practices that  
14 are unanticipated and do not fall into the scope of one of the conventional compatible practices to  
15 proceed without consent as long as data subjects substantially benefit from the practice. In order to  
16 find that data subjects substantially benefit from the practice, a court should ask whether data subjects  
17 would be likely to prefer that the processing occur and would be likely to consent to the processing if  
18 it were not for the transaction costs inherent to consenting processes.  
19

20 Practices that qualify as compatible under subsection (b)(10) include detecting and reporting  
21 back to data subjects that they are at some sort of risk, e.g. of fraud, disease, or criminal victimization.  
22 Another example is processing that is used to recommend other purchases that are complements or  
23 even requirements for a product that the data subject has already placed in a virtual shopping cart.  
24 Both of these examples are now routine practices that consumers favor, but when they first emerged,  
25 they seemed inappropriate. Subsection (b)(10) is intentionally reserving space, free from regulatory  
26 burdens, for win-win practices of this sort to emerge. This allowance for beneficial repurposing of  
27 data makes this act different in substance from the GDPR, which restricts data repurposing unless \_\_  
28 and which gives data subjects a right to object to any processing outside certain limited “legitimate  
29 grounds” of the controller. (Articles 5(1)(b), 18, and 22 of the General Data Protection Regulation.)  
30

31 The compatible data practice described in (b)(6) includes the use of personal data to initially  
32 train an AI or machine learning algorithm. The actual use of such an AI or machine learning  
33 algorithm in order to make a communication or decisional treatment must fall into one of the other  
34 categories of compatible data practices in order to be considered compatible.  
35

36 Subsection (c) makes clear that the act will not require pop-up windows or other forms  
37 of consent before using data for tailored advertising. This leaves many common web practices  
38 in place, allowing websites and other content-producers to command higher prices from  
39 advertisers based on behavioral advertising rather than using the context of the website alone.  
40 This marks a substantial departure from the California Consumer Privacy Act and other privacy  
41 acts that have been introduced in state legislatures, including the Washington Privacy Act Sec.  
42 103(5) and the proposed amendments to the Virginia Consumer Data Protection Act Sec. 59.1-  
43 573(5). All of these bills permit data subjects to opt out of the sale or disclosure of personal data  
44 for the purpose of targeted advertising.  
45

46 Under subsection (c), websites and other controllers cannot use or share data even in

1 pseudonymized form for tailored treatment unless tailoring treatment is compatible for an  
2 entirely different reason. For example, a firm that shares pseudonymized data with a third party  
3 controller for the purpose of creating “retention models” or “sucker lists” that will be used by  
4 the third party or by the firm itself to modify contract terms cannot rely on subsection (c),  
5 because the processing is used for targeted decisional treatment. The firm also cannot rely on  
6 subsection (b)(10) or any other provision of this section because the processing is unanticipated  
7 and does not substantially benefit the data subject. (See Maddy Varner & Aaron Sankin, *Sucker*  
8 *List: How Allstate’s Secret Auto Insurance Algorithm Squeezes Big Spenders*, THE MARKUP  
9 (February 25, 2020) for an allegation that provides an example of this sort of processing.) By  
10 contrast, a firm that runs a wellness-related app and shares pseudonymized data with a third  
11 party controller for the purpose of researching public health generally or for assessing a health  
12 risk to the data subject specifically would be in a different posture. Like the “sucker list”  
13 example, this controller might not be able to rely on subsection (c) because the processing may  
14 be used to guide a public health intervention or to modify recommendations that the wellness  
15 app gives to the data subject. Nevertheless, the app producer could rely on subsection (b)(10)  
16 for processing that changes the function of the app itself because this processing, while  
17 potentially unanticipated, redounds to the benefit of the data subject without meaningfully  
18 increasing risk of harm. The app producer could rely on subsection (b)(6) for disclosure of  
19 pseudonymized data to produce generalized research (which then may be used for general  
20 public health interventions.)

21  
22 Subsection (c) also clarifies that loyalty programs that use personal data to offer  
23 discounts or rewards are compatible practices. Although the targeted offering of discounts or  
24 rewards would constitute decisional treatment, these are accepted and commonly preferred  
25 practices among consumers. Indeed, most loyalty programs, including programs offering special  
26 rewards, premium features, discounts, or club-card privileges, would qualify as compatible  
27 practices under subsection (b)(1) since customers typically affirmatively subscribe or sign up  
28 for them in order to receive discounts and rewards.

29  
30 Subsection (d) incorporates any data practice that has been recognized as compatible through  
31 a voluntary consent process as one of the per se compatible data practices, effectively adding these to  
32 the list contained in subsection (c).

33  
34 **Section 8. Incompatible Data Practice**

35 (a) A controller or processor may engage in an incompatible data practice with the consent of  
36 the data subject as provided in subsections (b) and (c). A controller or processor engages in an  
37 incompatible data practice if:

- 38 (1) the processing is not a compatible data practice under Section 7 and is not a  
39 prohibited data practice under Section 9, or  
40 (2) is otherwise a compatible data practice but is inconsistent with a privacy policy

1 adopted under Section 6.

2 (b) A controller may process personal data that does not include sensitive data using an  
3 incompatible data practice if at the time personal data is collected about a data subject, the controller  
4 provides the data subject with notice and information sufficient to allow the data subject to  
5 understand the nature of the incompatible data processing and a reasonable opportunity to withhold  
6 consent to the practice.

7 (c) A controller may not process a data subject’s sensitive data for an incompatible data  
8 practice without the data subject’s express consent in a signed record for each practice.

9 (d) Unless processing is a prohibited data practice, a controller may require a data subject  
10 to consent to an incompatible data practice as a condition for access to the controller’s goods or  
11 services. The controller may offer a reward or discount in exchange for the data subject’s consent  
12 to process the subject’s personal data.

13 **Comment**

14  
15 An incompatible data practice is an unanticipated use of data that is likely to cause neither  
16 substantial harm nor substantial benefit to the data subject. (The former would be a prohibited data  
17 practice and the latter would be a compatible one.) An example of an incompatible data practice is a  
18 firm that develops an app that sells user data to third party fintech firms for the purpose of creating  
19 novel credit scores or employability scores.

20  
21 Subpart (d) makes clear that a firm may condition services on consent to processing that  
22 would otherwise be incompatible. In other words, if the business model for a free game app is to sell  
23 data to third party fintech firms, the app developers will have to receive consent that meets the  
24 requirements of subpart (d). But the firm can also refuse service to a potential customer who does not  
25 consent. This is distinguishable from the California Privacy Rights Act’s nondiscrimination provision,  
26 which permits variance in price or quality of service only if the difference is “reasonably related to the  
27 value provided to the business by the consumer’s data.” (California Privacy Rights Act Section 11.)

28  
29 **Section 9. Prohibited Data Practice**

30 (a) A controller may not engage in a prohibited data practice. Processing personal data  
31 is a prohibited data practice if the processing is likely to:

- 1 (1) subject a data subject to specific and significant:
- 2 (A) financial, physical, or reputational harm;
- 3 (B) embarrassment, ridicule, intimidation, or harassment; or
- 4 (C) physical or other intrusion on solitude or seclusion if the intrusion would
- 5 be highly offensive to a reasonable person;
- 6 (2) result in misappropriation of personal data to assume another's identity;
- 7 (3) constitute a violation of other law, including federal or state law against
- 8 discrimination;
- 9 (4) fail to provide reasonable data-security measures, including appropriate
- 10 administrative, technical, and physical safeguards to prevent unauthorized access; or
- 11 (5) process without consent under Section 8 personal data in a manner that is an
- 12 incompatible data practice
- 13 (b) It is a prohibited data practice to collect or create personal data by reidentifying or causing
- 14 the reidentification of pseudonymized or deidentified data unless:
- 15 (1) the reidentification is performed by a controller or processor that previously had
- 16 pseudonymized or deidentified the data;
- 17 (2) the data subject expects the personal data to be maintained in identified form by
- 18 the controller performing the reidentification; or
- 19 (3) the purpose of the reidentification is to assess the privacy risk of deidentified data
- 20 and the person performing the reidentification does not use or disclose reidentified personal data
- 21 except to demonstrate a privacy vulnerability to the controller or processor that created the
- 22 deidentified data.

23 **Comment**

24

1 Subsection 9(a) prohibiting certain practices applies to controllers. Under the act, it is  
2 controllers who determine the nature of processing activities.  
3

4 Reidentification of previously deidentified data is a prohibited practice unless the  
5 reidentification fits one of the exceptions in subsection (b). Exception (b)(1) covers controllers or  
6 processors that are in the practice of pseudonymizing personal data for security reasons and then  
7 reidentify the data only when necessary. This exception covers controllers or processors who already  
8 have the right and privilege to process personal data. Exception (b)(2) covers controllers who collect  
9 pseudonymized data from other controllers with the expectation that the data will be linked to the  
10 data subject's identity and maintained in identified form. An example is a credit card issuer that  
11 receives transaction data from a retailer in pseudonymized form (with card number, for example) and  
12 subsequently associates it with a specific individual's credit account for billing and other purposes.  
13 Exception (b)(3) exempts "white hat" researchers who perform reidentification attacks in order to  
14 stress-test the deidentification protocols. These researchers may disclose the details (without  
15 identities) of their demonstration attacks to the general public, and can also disclose the  
16 reidentifications (with identities) to the controller or processor.  
17

## 18 **Section 10. Data Privacy and Security Risk Assessment**

19 (a) A controller or processor shall conduct and maintain in a record a data privacy and  
20 security risk assessment. The assessment may take into account the size, scope and type of  
21 business of the controller or processor and the resources available to it. The assessment must  
22 evaluate:

23 (1) privacy and security risks to the confidentiality and integrity of the personal  
24 data being processed or maintained, the likelihood of the risks, and the impact that the risks  
25 would have on the privacy and security of the personal data;

26 (2) efforts taken to mitigate the risks; and

27 (3) the extent to which the data practices comply with this [act].

28 (b) The data privacy and security risk assessment must be updated if there is a change in  
29 the risk environment or in a data practice that may materially affect the privacy or security of the  
30 personal data.

31 (c) A data privacy and security risk assessment is confidential [and is not subject to a  
32 public records request or discovery in a civil action]. The fact that a controller or processor



1 conducted an assessment, the facts underlying the assessment, and the date of the assessment are  
2 not confidential.

3 **Legislative Note:** *The state should include appropriate language in subsection (c) exempting a*  
4 *data privacy assessment from an open records request and discovery in a civil case to the*  
5 *maximum extent possible under state law.*

6  
7  
8

**Comment**

9 The goal here is to ensure that all controllers and processors go through a reflective  
10 process of evaluation that is appropriate for their size and the intensity of data use. Other than  
11 being a record, the act does not require any particular format for the evaluation. There are many  
12 existing forms that companies can use to help them through a privacy impact assessment, and the  
13 Attorney General may recommend or provide some of these on their website.

14  
15  
16  
17  
18  
19  
20

Under this section, the privacy and risk assessment is a confidential document and should not be subject to disclosure or discovery. The purpose is to assure the assessment is an honest assessment rather than a document produced for possible future litigation. However, the fact that an assessment was completed and the date of that assessment are not confidential in order to permit enforcement of the section.

21

**Section 11. Compliance with Other Law Protecting Personal Data**

22 (a) A controller or processor complies with this [act] if it complies with a comparable  
23 personal-data protection law in another jurisdiction and the [Attorney General] determines the  
24 law in the other jurisdiction is equally or more protective of personal data than this [act]. The  
25 [Attorney General] may set a fee to be charged to a controller or processor that asserts compliance  
26 with a comparable law under this subsection. The fee must reflect the cost reasonably expected to be  
27 incurred by the [Attorney General] to determine whether the comparable law is equally or more  
28 protective than this [act].

29 (b) A controller or processor complies with this [act] with regard to processing that is  
30 subject to:

31 (1) the Health Insurance Portability and Accountability Act, Pub. L. 104-191, if  
32 the controller or processor is regulated by that act;

1 (2) the Fair Credit Reporting Act, 15 U.S.C. Section 1681 et seq.[, as amended],  
2 or otherwise is used to generate a consumer report by a consumer reporting agency as defined in  
3 603(f) of the Fair Credit Reporting Act, 15 U.S.C. Section 1681a(f)[, as amended], a furnisher of  
4 the information, or a person procuring or using a consumer report;

5 (3) the Gramm-Leach-Bliley Act of 1999, 12 U.S.C. Section 24a et. seq.[, as  
6 amended];

7 (4) the Drivers Privacy Protection Act of 1994, 18 U.S.C. Section 2721 et seq.[, as  
8 amended];

9 (5) the Family Education Rights and Privacy Act of 1974, 20 U.S.C. Section  
10 1232g[, as amended]; or

11 (6) the Children’s Online Privacy Protection Act of 1998, 15 U.S.C. Section 6501  
12 et seq.[, as amended.]

13 ***Legislative Note:*** *It is the intent of this act to incorporate future amendments to the cited federal*  
14 *laws. In a state in which the constitution or other law does not permit incorporation of future*  
15 *amendments when a federal statute is incorporated into state law, the phrase “as amended”*  
16 *should be omitted. The phrase also should be omitted in a state in which, in the absence of a*  
17 *legislative declaration, future amendments are incorporated into state law.*

18  
19

### Comment

20 Companies that collect or process personal data, particularly larger ones, have an interest  
21 in adopting a single set of data practices that satisfy the data privacy requirements of multiple  
22 jurisdictions. It is likely that such firms will adopt practices to meet the most demanding laws  
23 among the jurisdictions in which they do business. Compliance costs can be quite burdensome  
24 and detrimental to smaller firms that in the ordinary course of business must collect consumer  
25 data. The purpose of this section is to permit, in practice, firms to settle on a single set of  
26 practices relative to their particular data environment.

27

28 This section also greatly expands the potential enforcement resources for protecting  
29 consumer data privacy. Adoption of this act confers on the state attorney general, or other  
30 privacy data enforcement agency, authority not only to enforce the provisions of this act but also  
31 to enforce the provisions of any other privacy regime that a company asserts under subsection (a)  
32 as a substitute for compliance with this act.

33

1 The Attorney General is authorized to charge a reasonable fee for determining whether a  
2 particular law is equally or more protective than this act. It is assumed here that a reasonable  
3 consensus will be achieved within the enforcement community that will accept major  
4 comprehensive legislation as in compliance with this section. Accordingly, accepting the  
5 consensus would not require intensive activity by the Attorney General and would thus not result  
6 in a significant fee. Moreover, once another law was determined to be in compliance in a  
7 particular jurisdiction, it would not require further examination.  
8

9 Subsection (b) provides exemptions for processing subject to specific federal privacy  
10 regimes. Data practices that are not subject to federal regulations under the stated enactments are  
11 governed by this act. A firm that maintains personal data solely for processing covered by the  
12 scope of federal privacy laws identified in subsection (b) are deemed compliant with this entire  
13 Act. For example, a financial institution or medical facility that collects personal data and  
14 processes it for the purposes of delivery or billing related to financial or medical services is  
15 exempt from the obligations of the Act. But if the same firm processes personal data for the  
16 purpose of behavioral advertising, all of the notice, access, correction, and processing obligations  
17 of this Act will apply with respect to that processing.  
18

## 19 **Section 12. Compliance with Voluntary Consensus Standard**

20 A controller or processor complies with this [act] if it adopts and complies with a  
21 voluntary consensus standard recognized by the [Attorney General] under Section 15.

### 22 **Comment**

23  
24 Developing detailed common rules for data practices applicable to a wide variety of  
25 industries is particularly challenging. Data practices differ significantly from industry to  
26 industry. This is reflected in a number of specific federal enactments governing particular types  
27 of data (HIPPA for health information) or particular industries (Graham-Leach-Bliley for  
28 financial institutions). The Act imposes fundamental obligations on controllers and data  
29 processors to protect the privacy of data subjects. These include the obligations to allow data  
30 subjects to access and copy their data, to correct inaccurate data, to be informed of the nature and  
31 use of their data, to expect their data will only be used as indicated when it is collected, and to be  
32 assured there are certain data practices that are prohibited altogether. No voluntary consensus  
33 standard may undermine these fundamental obligations.  
34

35 On the other hand, how these obligations are implemented may depend on the particular  
36 business sector. Developing procedures for access, copying, and correction of personal data can  
37 be a complex undertaking for large controllers. And consumers have vastly different  
38 expectations about the use of their personal information depending on the underlying transaction  
39 for which their data is sought. Signing up for a loyalty program is far different than taking out a  
40 mortgage. Providing an opportunity for industry sectors, in collaboration with stakeholders  
41 including data subjects, to agree on methods of implementing privacy obligations provides the  
42 flexibility any privacy legislation will require. There is some experience, primarily at the federal  
43 level, of permitting industries to engage in a process to develop voluntary consensus standards  
44 that can be compliant with universal regulation and yet tailored to the particular industry.

1 An industry may adopt a comprehensive set of voluntary consensus standards to govern  
2 their privacy compliance policies or it may adopt a more specific standard that responds to one or  
3 more compliance requirements. For example, stakeholders of a particular industry may agree on  
4 the practices to be deemed “compatible practices” under this act, but leave other requirements to  
5 individual entity decision-making.  
6

7 Voluntary consensus standards are NOT to be confused with industry codes or other  
8 forms of self-regulation. Rather these standards must be written through a private process that  
9 assures that all stakeholders participate in the development of the standards. That process is set  
10 out in the following sections. Any concerns regarding self-regulation are also addressed in this  
11 act by requiring the Attorney General to formally recognize standards as being in substantial  
12 compliance with this Act. Thus there must be assurance that any voluntary consensus standard  
13 fully implements the fundamental privacy protections adopted by the act.  
14

15 The act creates a safe harbor for covered entities that comply with voluntary consensus  
16 standards, recognized by the state Attorney General, that implements the Act’s personal data privacy  
17 protections and information system security requirements for defined sectors and in specific contexts.  
18 These voluntary consensus standards are to be developed in partnership with consumers, businesses,  
19 and other stakeholders by organizations such as the American National Standards Institute, and by  
20 using a consensus process that is transparent, accountable and inclusive and that complies with due  
21 process. This safe harbor for voluntary consensus standards is modeled on Articles 40 and 41 of the  
22 GDPR, which provides for recognition of industry “codes of conduct,” the Consumer Product Safety  
23 Act (“CPSA”), 15 U.S.C. § 2056, *et seq.*, which uses voluntary consensus standards to keep  
24 consumer products safe, and the Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. § §  
25 6501-6506, which uses such standards to protect children’s privacy online. This provision of the Act  
26 is in conformity with the Office of Management and Budget (OMB) Circular A-119, which  
27 establishes policies on federal use and development of voluntary consensus standards. Thus there is  
28 not only precedent for the adoption of voluntary consensus standards but actual experience in doing  
29 so.  
30

31 By recognizing voluntary consensus standards, the Act provides a mechanism to tailor the  
32 Act’s requirements for defined sectors and in specific contexts, enhancing the effectiveness of the  
33 Act’s privacy protections and information system security requirements, reducing the costs of  
34 compliance for those sectors and in those contexts, and, by requiring that the voluntary consensus  
35 standard be developed through the consensus process of a voluntary consensus standards body, the  
36 concerns and interests of all interested stakeholders are considered and reconciled, thus ensuring  
37 broad-based acceptance of the resulting standard. Finally, by recognition of voluntary consensus  
38 standards by the Attorney General, the Act ensures that the voluntary consensus standard substantially  
39 complies with the Act.  
40

41 Voluntary consensus standards also provides a mechanism to provide interoperability between  
42 the act and other existing data privacy regimes. The Act encourages that such standards work to  
43 reasonably reconcile any requirements among competing legislation, either general privacy laws or  
44 specific industry regulations. For example, it would provide an opportunity for firms that process both  
45 financial, health, and other data to attempt to create a common set of practices that reconcile HIPPA  
46 and GLB regulations with that applicable under this act for other personal data.

1 **Section 13. Content of Voluntary Consensus Standard**

2 A stakeholder may initiate the development of a voluntary consensus standard for  
3 compliance with this [act]. A voluntary consensus standard may address any requirement of this  
4 [act], including:

- 5 (1) identification of compatible data practices for an industry;
- 6 (2) the procedure and method for securing consent of a data subject for an  
7 incompatible data practice;
- 8 (3) a common method for responding to a request by a data subject for access to  
9 or correction of personal data, including a mechanism for authenticating the identity of the data  
10 subject;
- 11 (4) a format for a privacy policy to provide consistent and fair communication of  
12 the policy to data subjects;
- 13 (5) practices that provide reasonable security for personal data maintained by a  
14 controller or processor; and
- 15 (6) any other policy or practice that relates to compliance with this [act].

16 **Comment**

17 This section clarifies the policies and practices that seem most appropriate for voluntary  
18 consensus standards and most likely to differ among industry sectors. The list of policies and  
19 practices is not intended to be exclusive. The section, however, does make clear that any such  
20 standards must remain consistent with the act’s privacy protection obligations on controllers and  
21 processors.

22  
23 **Section 14. Procedure for Development of Voluntary Consensus Standard**

24 The [Attorney General] may not recognize a voluntary consensus standard unless it is  
25 developed through a consensus procedure that:

- 26 (1) achieves general agreement, but not necessarily unanimity, and:

1 (A) includes stakeholders representing a diverse range of industry, consumer,  
2 and public interests;

3 (B) gives fair consideration to each comment by a stakeholder;

4 (C) responds to each good-faith objection by a stakeholder;

5 (D) attempts to resolve each good-faith objection by a stakeholder;

6 (E) provides each stakeholder an opportunity to change the stakeholder's vote  
7 after reviewing comments; and

8 (F) informs each stakeholder of the disposition of each objection and the  
9 reason for the disposition;

10 (2) provides stakeholders a reasonable opportunity to contribute their knowledge,  
11 talents, and efforts to the development of the standard;

12 (3) is responsive to the concerns of all stakeholders;

13 (4) consistently complies with documented and publicly available policies and  
14 procedures that provide adequate notice of meetings and standards development; and

15 (5) includes a right for a stakeholder to file a statement of dissent.

16 **Comment**

17 This section outlines the process required for the adoption of voluntary consensus  
18 standards in order to allow them to be considered a safe harbor under this act. The process is  
19 consistent with OMB A-119 and has been utilized by industries and accepted by federal  
20 regulatory agencies. The development and operation of the process required by this section is  
21 the responsibility of the voluntary consensus organization that facilitates development of the  
22 standards. The role of the Attorney General would be only to assure that the resulting standards  
23 were developed by such a process.

24  
25 **Section 15. Recognition of Voluntary Consensus Standard**

26 (a) On filing of a request by any person, the [Attorney General] may recognize a voluntary  
27 consensus standard if the [Attorney General] finds the standard:

- 1 (1) substantially complies with any requirement of Sections 5 through 10;
- 2 (2) is developed through a procedure that substantially complies with Section 14 of
- 3 this [Act]; and
- 4 (3) reasonably reconciles a requirement of this [act] with the requirements of other
- 5 law.

6 (b) The [Attorney General] shall adopt rules under [cite to state administrative procedure act]  
7 that establish a procedure for filing a request under subsection (a) to recognize a voluntary consensus  
8 standard. The rules may:

9 (1) require the request to be in a record demonstrating that the standard and procedure  
10 through which it was adopted comply with this [act];

11 (2) require the applicant to indicate whether the standard has been recognized as  
12 appropriate elsewhere and, if so, identify the authority that recognized it; and

13 (3) set a fee to be charged to the applicant, which must reflect the cost reasonably  
14 expected to be incurred by the [Attorney General] in acting on a request.

15 (c) The [Attorney General] shall determine whether to grant or deny the request and provide  
16 the reason for a denial. In making the determination, the [Attorney General] shall consider the need  
17 to promote predictability and uniformity among the states and give appropriate deference to a  
18 voluntary consensus standard developed consistent with this [act] and recognized by a privacy-  
19 enforcement agency in another state.

20 (d) After notice and hearing, the [Attorney General] may withdraw recognition of a voluntary  
21 consensus standard if the [Attorney General] finds that the standard or its implementation is not  
22 consistent with this [act].

23 (e) A voluntary consensus standard recognized by the [Attorney General] is a public record

1 under [cite to state public records law].

2 **Comment**

3 This section makes clear that the basic privacy interests of consumers will be protected  
4 throughout any voluntary consensus standards process. Each state Attorney General or other data  
5 privacy enforcement agency must assure that the rights accorded to consumers under this Act with  
6 respect to their personal data are preserved. To be recognized as compliant with this act, the Attorney  
7 General must determine that the standards were adopted through a process outlined in Section [ ],  
8 which will assure that all stakeholders including representatives of data subjects are involved. The  
9 Attorney General must also confirm that the standards are consistent with the act's imposed  
10 obligations on controllers and processors. And the Attorney General must find the standards  
11 reasonably reconcile other competing data privacy regimes.

12  
13 Any industry or firm seeking to establish a set of voluntary consensus standards would have  
14 the burden of convincing the Attorney General that the standards comply with this section. It is  
15 recognized that this standard setting process can be expensive and thus the incentive for particular  
16 industries to participate will be determined in part by their expectation that standards will be treated  
17 consistently from state to state. Thus, the act contains provisions that encourage the Attorney General  
18 of each state in which this act is adopted to collaborate with Attorneys General from other states.

19  
20 The Attorney General is encouraged to work with other states to achieve some uniformity of  
21 application and acceptance of these standards. While the act recognizes the State's inherent right to  
22 determine the level of data privacy protection it does encourage the Attorney General to take the  
23 actions of other states into account.

24  
25 Currently the National Association of Attorneys General has created a forum through which  
26 various state Attorney Generals offices share policies and enforcement actions related to consumer  
27 protection including specifically data privacy. This activity suggests it is realistic to believe that  
28 consistency across states can be achieved.

29  
30 The section also authorizes the Attorney General to charge a fee commensurate with the  
31 expense of reviewing requests for recognition of voluntary consensus standards. Such a fee is  
32 appropriate to assure adequate resources for this process and as a cost of seeking a safe harbor from  
33 otherwise applicable legislation.

34  
35 **Section 16. Applicability of [Consumer Protection Act]**

36 (a) Subject to subsection (b), the enforcement and remedies under [cite to state consumer  
37 protection act] apply to a violation of this [act].

38 (b) A knowing violation of this [act] is subject to the remedies, penalties, and authority  
39 under the [cite to state consumer protection act]. A person that engages in conduct that has been



1 determined by the [Attorney General] or a court to be a prohibited data practice or an  
2 incompatible data practice without the consent of the data subject as required by Section 8, is  
3 presumed to have violated this [act] knowingly. Any other violation of this [act] is subject to  
4 enforcement by injunctive relief or a cease and desist order.

5 (c) The [Attorney General] may adopt rules under [cite to state administrative procedure  
6 act] to implement this [act].

7 (d) In adopting rules under this section, the [Attorney General] shall consider the need to  
8 promote predictability for data subjects and regulated entities and uniformity among the states  
9 consistent with this [act]. The [Attorney General] may:

10 (1) consult with Attorneys General or other personal-data-privacy-enforcement  
11 agencies in other jurisdictions that have an act substantially similar to this [act];

12 (2) consider suggested or model rules or enforcement guidelines promulgated by  
13 the National Association of Attorneys General or any successor organization;

14 (3) consider the rules and practices of Attorneys General or other personal-data-  
15 privacy-enforcement agencies in other jurisdictions; and

16 (4) consider voluntary consensus standards developed consistent with this [act],  
17 that have been recognized by other Attorneys General or other personal-data-privacy-  
18 enforcement agencies.

19 [(e) In an action or proceeding to enforce this Act by the [Attorney General] in which the  
20 [Attorney General] prevails, the [Attorney General] may recover reasonable expenses and costs  
21 incurred in investigation and prosecution of the case.]

22 **Legislative Note:** *Include subsection (e) only if the state's applicable consumer protection act*  
23 *does not provide for the recovery of costs and attorney's fees.*

24  
25

#### Comment

1 The challenge in uniform state legislation when agencies are given the power to adopt  
2 implementing rules and regulations is to continue to assure a reasonable degree of uniform  
3 application and enforcement of the substantive provisions. This is not a unique problem here  
4 where the state Attorney General or any other personal data privacy enforcement agency will be  
5 required to implement and enforce standards that are, by their nature, flexible so they may be  
6 implemented by diverse industries. Nor is this a problem limited to data privacy protection.  
7 Every state has adopted a general consumer protection law that governs transactions of interstate  
8 businesses within the state. The enforcement provision here is modeled after these “little FTC  
9 acts” and merely provides detail and specificity related to data privacy.

10  
11 What remains uniform by adopting this act is the acknowledgement of the rights of  
12 consumers to obtain access to data held about them, to correct inaccurate data, and to be  
13 informed of the uses to which their data may be put. The distinction in this act between  
14 compatible, incompatible, and prohibited uses of personal data would create a uniform approach  
15 to the use of personal data although the very concept of “compatible” use is dependent on the  
16 nature of the underlying transaction from which the data is collected.

17  
18 In order to encourage as much uniformity as possible, the state Attorney General is  
19 encouraged by subsection (c) to attempt to harmonize rules with those in other states that have  
20 adopted this act. The Attorney General may also consider voluntary consensus standards that  
21 have been approved in other states, but, of course, there is no requirement that he accept them  
22 unless they have been previously approved in this state. These provisions are derived from  
23 section 9-526 of the Uniform Commercial Code which has been successful in harmonizing the  
24 filing rules and technologies for security interests by state filing offices. While there is not a  
25 direct analogy between privacy enforcement and filing rules, the potential, it demonstrates that  
26 legislation can successfully encourage state officials to cooperate as a substitute for federal  
27 dictates.

28  
29 The section applies to general policies and not to the decision to bring a particular  
30 enforcement action. The latter decision is one for prosecutorial discretion.

31  
32 Subsection (e) allows the Attorney General to recover the reasonable costs of  
33 investigation and prosecution of cases under this act if the Attorney General prevails. Attorneys  
34 fees are not included because in most instances those are the salaries of regular office legal staff.  
35 However, the salary costs associated with a particular case would be included in the reasonable  
36 costs of investigation and prosecution. A comparable provision was adopted in Virginia.

37  
38 Many states have adopted some form of private remedy for some violations of their  
39 consumer protection acts. In some states private causes of action are authorized only for  
40 violations of established rules rather than the general prohibition against unfair or deceptive acts.  
41 Others may impose procedural requirements such as requiring plaintiffs to engage with the  
42 Attorney General before bringing a suit. See, National Consumer Law Center, *Unfair and*  
43 *Deceptive Acts and Practices* (9<sup>th</sup> ed. 2016). As section 17 makes clear, this act defers to existing  
44 state law and practice with regard to whether this act creates a private cause of action. But even  
45 in states that allow for private causes of action, the plaintiffs must be prepared to show that the  
46 violation was a knowing violation which will generally require the plaintiffs to show that the

1 defendant had notice that the practice or omission that they committed was illegal. Nothing in  
2 this act is intended to displace traditional common law or other statutory remedies invasions of  
3 privacy or other wrongs.

4  
5 **Section 17. Limits of Act**

6 This [act] does not create or affect a cause of action under other law of this state.

7 **Comment**

8  
9 The use of personal data can be implicated in traditional causes of action for defamation,  
10 right to privacy, intentional infliction of emotional suffering, or similar actions. In some states  
11 these actions remain at common law; in others they are creates of statutes. This section assures  
12 that those causes of action remain unaffected by this act.

13  
14 **Section 18. Uniformity of Application and Construction**

15 In applying and construing this uniform act, a court shall consider the promotion of  
16 uniformity of the law among jurisdictions that enact it.

17 **Section 19. Electronic Records and Signatures in Global and National Commerce**

18 **Act**

19 This [act] modifies, limits, or supersedes the Electronic Signatures in Global and National  
20 Commerce Act, 15 U.S.C. Section 7001 et seq.[ as amended], but does not modify, limit, or  
21 supersede 15 U.S.C. Section 7001(c), or authorize electronic delivery of any of the notices  
22 described in 15 U.S.C. Section 7003(b).

23 **[Section 20. Severability**

24 If a provision of this [act] or its application to a person or circumstance is held invalid,  
25 the invalidity does not affect another provision or application that can be given effect without the  
26 invalid provision.]

27 *Legislative Note: Include this section only if the state lacks a general severability statute or a*  
28 *decision by the highest court of this state adopting a general rule of severability.*

29  
30 **Section 21. Effective Date**

1            This [act] takes effect [180 days after the date of enactment].

2    ***Legislative Note:*** *A state may wish to include a delayed effective date to allow time for affected*  
3    *agencies and industry members to prepare for implementation and compliance.*