D R A F T

FOR DISCUSSION ONLY

# COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT

NATIONAL CONFERENCE OF COMMISSIONERS

ON UNIFORM STATE LAWS

April 24, 2020 Drafting Committee Meeting

Redline Draft



*The ideas and conclusions set forth in this draft, including the proposed statutory language and any comments or reporter's notes, have not been passed upon by the National Conference of Commissioners on Uniform State Laws or the drafting committee. They do not necessarily reflect the views of the Conference and its commissioners and the drafting committee and its members and reporter. Proposed statutory language may not be used to ascertain the intent or meaning of any promulgated final statutory proposal.*

April 21, 2020

**COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA 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, *Chair* |
| 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. TENNESSEN | Minnesota |
| KERRY TIPPPER | Colorado |
| ANTHONY C. WISNIEWSKI | Maryland |
| CANDACE M. ZIERDT | Florida |
| DAVID V. ZVENYACH | Wisconsin |
| CARL H. LISMAN | Vermont, *President* |
| WILLIAM H. HENNING | Alabama, *Division Chair* |

**OTHER PARTICIPANTS**

| | |
|---|---|
| WILLIAM McGEVERAN | Minnesota, *Reporter* |
| MICHAEL AISENBERG | Virginia, *American Bar Association Advisor* |
| STEVEN L. WILLBORN | Nebraska, *Style Liaison* |
| TIM SCHNABEL | Illinois, *Executive Director* |

Copies of this act may be obtained from:

NATIONAL CONFERENCE OF COMMISSIONERS
ON UNIFORM STATE LAWS
111 N. Wabash Ave., Suite 1010
Chicago, Illinois 60602
312/450-6600
www.uniformlaws.org

**COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT**

**TABLE OF CONTENTS**

**COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT**

**SECTION 1. SHORT TITLE.** This [act] may be cited as the Collection and Use of Personally Identifiable Data Act.

**SECTION 2. DEFINITIONS.** In this [act]

(1) "Data controller" or "controller" means a person who, alone or jointly with others, determines the purposes and means~~, and~~ of processing ~~of~~ personal data.

~~(2) "Data custodian" or "custodian" refers to both data controllers and data processors who have possession or control of personal data or deidentified data.~~

(3) "Data processor" or "processor" means a person who processes personal data on behalf of a data controller and under that data controller's direction.

(4) "~~Data subject~~Consumer" means the identified or identifiable individual~~, device, or household~~ to whom personal data refers. It does not include an individual acting in a commercial context, such as acting as an employee, officer, director, agent, or contractor of a commercial, non-profit, or government entity.

(5) "Deidentified" means that ~~the~~ technical, organizational, or administrative safeguards have been applied so that information cannot ~~capacity of information to~~ identify, describe, or be associated with any particular ~~data subject~~consumer ~~individual, device, or household~~ ~~has been eliminated~~, provided the ~~custodian~~ controller of the information makes no attempt to ~~restore the capacity of the information to~~ re-identify, ~~describe,~~ or be associate~~d~~ with any particular consumer ~~data subject reidentify the information~~ and implements the following measures to prevent others from doing so:

(A) Technical safeguards that reasonably prevent reidentification of the ~~individual, device, or household~~~~data subject~~ consumerto whom the information may pertain;~~.~~

**Commented [KA1]:** Consistent with CCPA, this model should focus on individuals acting as consumers only, and exclude B2B and Employee data, as those exponentially increase operational complexity with little increase in privacy protection.

**Commented [KA2]:** It is unrealistic to set a standard that the capacity for reidentification has been completely eliminated, and this standard is contrary to the Obama FTC standard. Instead, we have suggested amendments to ensure that controls are in place to prevent reidentification.

(B) Business processes that specifically prohibit reidentification of the information; and

(C) Business processes that are reasonably designed to prevent inadvertent release of deidentified data.

~~(6) "Device" means any physical object that connects to the internet or to another device. Data related to a device, including unique identification numbers and IP addresses, is personal data if it can be associated with a particular data subject by using a reasonable amount of effort.~~

(7) "Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(8) "Person" means an individual, estate, business or nonprofit entity, or other legal entity. The term does not include a public corporation, government or governmental subdivision, agency, or instrumentality.

(9) "Personal data" means information that identifies or describes a particular ~~individual data subject~~consumer and information that can be associated with a particular ~~individual~~ data consumer ~~subject~~ by using a reasonable amount of effort. ~~Personal data need not have been collected directly from a data subject. Probabilistic inferences about an individual, including inferences derived from profiling, are included in the definition of personal data.~~ Information that identifies a household or a device is personal ~~date~~ data if it can be associated with a particular ~~individual data subject~~consumer by using a reasonable amount of effort. Deidentified data, aggregate data, and publicly available information are ~~is~~ not personal data.

(10) "Processing " means any operation performed on personal data , whether or not by automated means, including use, storage, disclosure, analysis, ~~and~~ or modification.

(11) "Profiling " means any form of solely automated processing ~~of~~ of individual personal

**Commented [KA3]:** The definition of "personal data" already specifies the circumstances under which device-level data is personal data. The term "device" is not used anywhere else in the text, so a specific definition does not make sense here.

**Commented [KA4]:** Since profiling is separately defined below, this statement is unnecessary.

data elements that are combined in order to evaluate, analyze, or predict a ~~data subject's~~consumer's economic status, health, demographic characteristics (including race, gender, or sexual orientation), personal preferences, interests, character, reliability, behavior, or social or political views~~, physical location, or movements~~. Profiling does not include evaluation, analysis, or prediction based solely on a ~~data subject~~consumer's current activity, including search queries, if no personal data is retained for future use after the completion of the activity. Probabilistic inferences derived from profiling are personal data.

(12) "Publicly available data " means information that has been made available from federal, state, or local government records in accordance with law~~, provided the information is being used in a manner consistent with any conditions on its use imposed by law~~.

(13) "Sensitive data" means

(A) ~~personal data revealing~~ racial or ethnic origin, religious beliefs, mental or physical health ~~condition or~~ diagnosis, sexual orientation or identity, ~~activities or preferences related to gender or sexuality,~~ or citizenship or immigration status;

(B) biometric and genetic data; and

(C) personal data ~~about~~ from a ~~data subject~~consumer who is known to be under [13] years of age.

~~(14) "Sign" means, with present intent to authenticate or adopt a record:~~

~~(A) to execute or adopt a tangible symbol; or~~

~~(B) to attach to or logically associate with the record an electronic symbol, sound, or process.~~

(15) "State" means a state of the United States, the District of Columbia, Puerto Rico, the United States Virgin Islands, or any territory or insular possession subject to the jurisdiction of

**Commented [KA5]:** Profiling is *not* the collection of individual data elements – rather, it is the combination of such elements to evaluate, analyze, predict, etc.

**Commented [KA6]:** This would sweep in simple address information, as well as any fitness tracker, which are not truly profiling.

**Commented [KA7]:** A similar provision was removed from the CCPA in 2019 amendments because of concern that restrictions on use of this information violate the First Amendment.

**Commented [HJ8]:** Health condition is somewhat overbroad, as it can include current symptoms, like a statement by an individual has a cold.

**Commented [KA9]:** This is a critical change that aligns the ULC draft with COPPA. State laws that are inconsistent with COPPA are preempted by it.

the United States. [The term includes a federally recognized Indian tribe.]

(16) "Targeted advertising" means advertising displayed to a ~~data subject~~consumer where the advertisement is selected based on personal data obtained from a consumer's activities over time and across online applications or sites of unaffiliated third parties on the basis of profiling to predict such consumer's preferences or interests~~.~~

(17) "Third Party" means a person, private entity, public entity, agency, or other body other than the consumer, ~~covered entity~~controller, processor, joint venture, or affiliate of the ~~covered entity~~controller.

(17) "Transfer" means to convey personal data into the possession or control of another ~~custodian~~controller or third party.

Comment

The definition of "personal data" includes any information that incorporates specific personal identifiers, including name; a unique identification number such as a social security number; an individual number for financial or similar accounts; payment card information; a postal address; a telephone number; or an email address. The definition is not limited to such directly identifying informaton, however. A profile about a unique data subject may be personal data even if it lacks any of these traditional identifiers. When information can be used to make an association with a data subject through one or more intervening inferences using a reasonable amount of effort, that information qualifies as personal data. Similarly, information associated with a device or a household is personal data if it can be associated with a particular data subject, even if the name of that data subject is not known to the relevant data controller or processor.

**SECTION 3. SCOPE.**

(a) This Act applies to the commercial activities of a person who conducts business [in the State of X] or produces products or provides services targeted to [the State of X], provided that the person:

(1) is the ~~custodian~~ controller of personal data concerning more than [250,000] ~~individuals, devices, or households~~~~data subjects~~ consumers ~~in one year~~, or sensitive personal information of more than [25,000] consumers in the previous year.

**Commented [KA10]:** We have modified this definition to align with the NAI privacy standard that has been in use for several years to facilitate consumer control; our edited definition was also in WPA and was not controversial.

**Commented [KA11]:** We have added this definition to help the framework account for entities that are not Controllers or Processors, but nonetheless may receive or provide personal data. The CCPA has this concept.

**Formatted:** Centered

**Formatted:** Line spacing: single

**Commented [KA12]:** To truly exempt small businesses, a much larger number than 50,000 is needed.

~~(2) earns more than [50] percent of its gross annual revenue directly from its activities as a controller or processor of personal data,~~ or

(3) is a data processor acting on behalf of a data controller whose activities the data processor knows ~~or has reason to know~~ satisfy the requirements of this section.

(b) This Act does not apply to

(1) personal health information or deidentified information as defined under the Health Information Portability and Accountability Act [CITE] [and regulations] when the ~~custodian~~ controller or processor of that data is regulated by that statute.

(2) an activity involving ~~personal~~ information governed by the Fair Credit Reporting Act, section 1681 et seq., Title 15 of the United States Code, or otherwise used to generate a consumer report, by a consumer reporting agency, as defined by 15 U.S.C. Sec. 1681a(f), by a furnisher of information, or by a person procuring or using a consumer report.

(3) publicly available information. ~~For purposes of this section, publicly available information means information that is lawfully made available from federal, State, or local government records, or generally accessible or widely distributed media.~~

(4) ~~personal information collected, processed, sold, or disclosed by~~ a financial institution or information subject to Title V of ~~as defined by 15 U.S.C. § 6809(3) pursuant to~~ the federal Gramm-Leach-Bliley Act of 1999 (~~Public Law 106-102~~15 U.S.C. 6801 et seq., and the applicable rules and regulations promulgated thereunder).

(5) information regulated by the Federal Family Educational Rights and Privacy Act, 20 U.S.C. 1232 and its implementing regulations.

(6) personal data collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq).

**Commented [HJ13]:** This clause would cover a very broad range of small IT businesses.

**Commented [KA14]:** This is an important addition to recognize that HIPAA has its own standard for deidentification and avoid confusingly and arbitrarily regulating information that is de-identified in accordance with HIPAA.

(~~5~~6) ~~This [act] does not apply to~~ state or local government entities.

(~~6~~7) Personal data collected or retained by an employer with regard to its employees or contractors that is directly related to the employment relationship or personal data collected or retained in the course of, or for the purpose of, providing or receiving a product or service to or from a person acting on behalf of a business, non-profit, or government entity.

(~~7~~8) The [Attorney General] may by regulation exempt other information or transactions from this Act or a portion of this act, provided the ~~collection,~~ processing, transfer, or retention of the information is regulated by other law.

(c) Nothing in this act shall prevent the ~~collection, authentication, maintenance, retention, disclosure, sale,~~ processing~~, communication, or use~~ of personal ~~information~~ data necessary to:

(1) Initiate or ~~C~~complete a transaction in goods or services that the ~~data subject~~consumer requested.

(2) Engage in routine business practices necessary to provide, maintain, or improve the controller's or processor's products or services

(~~2~~3) Protect against, prevent, detect, investigate, report on, prosecute, or remediate actual or potential:

(i) Fraud, harassment, identity theft, or threats to the integrity or security of systems;

(ii) Unauthorized transactions or claims;

(iii) Security incidents;

(iv) Malicious, deceptive, or illegal activity; or

(v) Other legal liability;

**Commented [HJ15]:** This is a B2B exception based upon the CCPA moratorium. It would not be necessary if the definition of "personal information" is limited to true consumer data.

**Commented [KA16]:** This is a concise acknowledgment of the principle that businesses have core routine operations (billing, shipping, network maintenance, etc.) that consumers expect to occur, and that this act should not frustrate. The exception is entirely consistent with the 2012 FTC staff report and Obama White House Privacy white paper.

**Formatted:** Indent: Left: 0.5", First line: 0.5"

(~~3~~4) Assist another person, entity, or government agency in conducting any of the activities specified in subsections (1 or 2); or

(~~4~~5) Comply with or defend claims under federal, state, or local laws, regulations, rules, guidance, or recommendations:

(i) Setting requirements, standards, or expectations to limit or prevent corruption, money laundering, export controls; or

(ii) Related to any of the activities specified in subsection (~~1~~2) of this subsection.

(d) Nothing in this act shall require the controller or processor to:

(1) Undertake actions that would compromise the privacy, security, or other rights of the personal data of another consumer (for example, when exercising rights would give a person access to someone else's information);

(2) Undertake actions that are technically infeasible under the circumstances, or, with regard to information that is in an archived or backup system or in unstructured format, to locate and retrieve information that is technically impracticable to locate or retrieve;

(3) Disclose trade secrets or proprietary technology;

(4) Re-identify or otherwise link information that is not already maintained in a manner that would be considered personal data; or

(5) Violate federal or state law or the rights and freedoms of other individuals, including under the [STATE] or United States Constitution.

**SECTION 4. ~~DATA SUBJECT'S~~CONSUMER RIGHTS.** ~~Data subjects~~Consumers may exercise, as provided in this Act, the following rights with respect to their personal data, subject to the provisions in section 3:

**Commented [KA17]:** We have added common-sense exceptions here that focus on security, legal compliance, revealing proprietary technology, and technically infeasible processes.

**Commented [HJ18]:** This exception is very important to make compliance with data deletion, data access and other rights that are operationally highly complex. Businesses sometimes receive bits of personal information from as many as eight different channels. Locating these data in unstructured format or in back-up systems that are not practical to retrieve is counter to privacy, because it requires making data *more retrievable, which means that it will be used more*.

**Commented [HJ19]:** This is a CCPA exception that avoids foreign government and corporate spies trying to leverage these rights to conduct espionage.

(1) The right to have a data controller confirm whether or not the controller has retained or is processing the ~~data subject's~~consumer's personal data.

(2) The right to be provided by a data controller of a copy of the ~~data subject's~~consumer's personal data in accordance with section 5 of this act.

(3) The right to have a data controller correct inaccuracies in the ~~data subjects~~consumer's personal data retained or processed by the data controller, taking into account the nature of the personal data and the purposes of processing of the personal data.

(4) ~~Subject to section 3 of this Act, t~~~~The~~The right~~, subject to section 3~~, to have the data controller delete the ~~data subject~~consumer's personal data.

**SECTION 5. ~~DATA SUBJECT'S~~CONSUMER'S RIGHT TO A COPY OF PERSONAL DATA.**

(a) In implementing the ~~data subject's~~consumer's right to a copy of personal data held by the data controller, the following rules apply:

(1) Upon ~~request~~receipt of a verifiable request, a data controller must provide a ~~data subject~~consumer with a copy of the ~~data subject's~~consumer's personal data once per calendar~~year~~ free of charge.

(2) The data controller may charge a reasonable fee based on actual administrative costs to comply with additional requests.

(3) If requests by a ~~data subject~~consumer are manifestly unreasonable or excessive, the data controller may refuse to act on the requests for one year.

(4) The consumer may submit a verifiable request that, for personal data ~~If the data controller collected the data subject's personal data~~ collected directly from the ~~data subject,~~ consumer, the copy should, to the extent ~~technically feasible~~practicable, ~~be provided in a way~~

**Commented [KA20]:** While seemingly a simple concept, the explosion of user-generated content and the subjectiveness of "inaccurate" information makes the right to correction one of the most operationally complex rights to implement. This clause would give the controller needed flexibility.

**Commented [HJ21]:** Section 3 qualifies all rights, not just Section 4.

**Commented [HJ22]:** Verification of requests is critical to prevent pretexting. The CCPA regs focus heavily on this risk.

~~that would~~ enable~~s~~ the ~~data subject~~consumer to transmit the data to another data controller by automated means.

**SECTION 6. RIGHTS RELATED TO TARGETED ADVERTISING AND PROFILING.**

(a) A ~~data subject~~consumer has the right ~~to restrict~~ to opt out of a data controller ~~from~~ processing or transfer~~-~~ring personal data pertaining to the ~~data subject~~consumer (an "opt out") for purposes of

(1) targeted advertising;

(2) profiling in furtherance of decisions by the controller that result in a provision or denial of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities~~, such as food and water~~.

~~(b) If a controller processes or transfer s sensitive data for the purposes listed in subsection (a), the controller must receive affirmative consent (an "opt in") from the data subject~~consumer ~~before undertaking such processing or transfer.~~]

**SECTION 7. ~~DATA SUBJECT~~CONSUMER RIGHTS GENERALLY.**

(a) A ~~data subject~~consumer may exercise rights under section 4 of this act by ~~notifying~~ providing a verifiable request to the controller by any reasonable means that the controller has established~~s~~ of the ~~data subject's~~consumer's intent to exercise one or more of these rights. Parents of a [minor child] may exercise these rights on behalf of the [minor child].

(b) A data controller shall comply with a verified request~~s~~ without undue delay. If the data controller has not complied with the request within [45 days] [a reasonable time] of receiving it, the data controller shall notify the ~~data subject~~consumer who made the request and

**Commented [KA23]:** There is no state precedent for this type of opt-in, and we believe it will likely confuse consumers to provide rights to opt out in some circumstances, and rights to opt-in to others.

**Commented [KA24]:** It is critical for both consumer and controller/processor security that the controller be able to authenticate the consumer making the request. Otherwise the statute becomes a vehicle for fraud and identity theft by hackers.

shall provide an explanation of the expected time to ~~actions being taken to~~ comply with the request.

(c) A data controller shall make reasonable efforts to ensure that its responses to requests by ~~data subjects~~consumers to exercise rights under this [act] include personal data in the possession or control of data processors acting on the controller's behalf. The data controller shall make reasonable efforts to notify processors acting on its behalf when ~~a data subject~~a consumer has exercised these rights, and shall instruct the processor to adjust the ~~data subject's~~consumer's personal data which is in the processor's possession to be consistent with the controller's response to the ~~data subject~~consumer's request.

(d) A data controller shall adopt ~~a Privacy Commitment pursuant to section 8 of this act which will describe the~~ procedures to be used in exercising the rights under this act. The data privacy officer for a data controller shall approve such ~~commitment~~procedures. An explanation of the procedures in clear language shall be reasonably accessible to all ~~data subjects~~consumers. The procedures shall include an opportunity to appeal an initial determination by the data controller. Appeals of an initial determination shall be reviewed under the supervision of the data privacy officer. ~~If a data subject is dissatisfied with the final disposition of an appeal, the data processor shall inform the data subject of the procedure to [file a complaint] with the [Attorney General].~~

**Commented [HJ25]:** Procedures are not an appropriate subject for a commitment that must be filed with the AG's Office. In fact, publishing the procedures would result in hackers and fraudsters studying them to figure out how to evade security measures that are embodied as part of the procedures.

**SECTION 8. DATA PRIVACY COMMITMENT.**

(a) A data controller who ~~collects, uses,~~ processes ~~or retains~~ personal data of a ~~data subject~~consumer, ~~shall file with the [Attorney General] a data privacy commitment. Such commitment~~ shall publish in its privacy policy ~~set forth~~ the following commitment, consistent with the requirements of this Act:

**Commented [JH26]:** The Commitments should be posted on a website (but should not include procedures for reasons explained above). Separate filings with each state AG would be a needless bureaucratic burden and would catch most controllers and processors unaware. They would also result in delaying innovation and improvements in procedures until filings were made with each State AG's Office.

~~(1) The precise method by which a data subject may communicate with the data controller in order to exercise the rights stated in Section 4.~~

~~(2) The manner and extent to which the person intends to use or transfer to others the personal data of data subjects, the purposes of such use or transfer, and a simplified method by which the data subject can withdraw consent for such use or transfer as authorized by this act.~~

(3) The manner in which the ~~person~~ controller intends to respond to verifiable consumer rights requests ~~a data subjects request for correction of personal data~~ including any policy to authenticate the request and to notify any data processor who possesses the personal data of such verifiable request ~~to make the correction~~.

~~(4) The manner by which the person intends to respond to a data subjects request to delete personal data.~~

(5) Any conditions on the exercise of the rights made necessary by the nature of the data controller's business or industry provided that those conditions do not unreasonably limit the substance of the rights ~~are not adversely affected~~.

(b) A person ~~who files a data privacy commitment~~ shall ~~also~~ publish the commitment in a conspicuous location on the person's website or mobile application, or, if the entity operates primarily through direct, physical transactions with consumers, a point where such direct transactions occur. ~~on its website and other points where it will be reasonably accessible to data subjects. transactions between the data subject and the data controller take place.~~

(c) The [Attorney General] may at any time ~~review the privacy commitment of any person and may~~ institute a regulatory action ~~to determine whether the commitment represents an unfair or deceptive practice in that it does not provide reasonable protection for a data subject's~~

**Commented [JH27]:** Items 1 and 2 are already addressed in the privacy policy section.

**Commented [JH28]:** This plenary, state-by-state authority is unworkable and contrary to the goals of a uniform state law.

~~privacy or the subject's rights with regard to its personal data as provided in this Act.~~pursuant to ~~Section 19~~[STATE UDAP ACT] to determine whether the ~~commitment~~data controller ~~satisfies~~is in material compliance with the provisions of this Act.

**SECTION 9. ~~CUSTODIAN'S~~ CONTROLLER'S ~~AND~~OR PROCESSOR'S ~~DUTY~~ RESPONSIBILITY OF LOYALTY.**

(a) A data ~~custodian~~ controller or processor shall not engage in processing practices that are unfair or materially ~~,~~deceptive~~, or abusive~~[REFERENCE STATE UDAP LANGUAGE]. An unfair practice shall include processing or use of data that exposes the ~~data subject~~consumer to an unreasonable ~~material~~ risk of material harm that is not outweighed by benefits to consumers or competition that the processing produces, and that consumers could not have reasonably avoided.

~~(b) The [Attorney General] may adopt regulations declaring particular processing practices to be unfair, deceptive, or abusive.~~

(c) A violation of subsection (a) shall be subject to regulatory enforcement under section 19.

(d) A data ~~custodian~~ controller or processor who engages in a practice after the final decision in the regulatory enforcement action that the practice is unfair, deceptive, or abusive under subsection (b) shall be subject to civil contempt remedies under the law of this State. ~~a private cause of action by a data subject under section 20.~~

**SECTION 10. ~~CUSTODIAN'S~~ CONTROLLER'S ~~AND~~OR PROCESSOR'S ~~DUTY~~ RESPONSIBILITY OF DATA SECURITY.**

(a) A data ~~custodian~~ controller or processor shall adopt, implement, and maintain reasonable data security measures to protect the confidentiality and integrity of personal data in

**Commented [KA29]:** The term "duty" is fraught with legal implications conflicting with traditional fiduciary duty that would needlessly complicate the goal of these obligations. For the same reason, this term was removed in similar WPA statutory language. "Responsibility" or "obligation" are clearer terms.

**Commented [HJ30]:** This is the FTC unfairness standard. Risks need to be weighed against benefits.

**Commented [KA31]:** This is far too broad a mandate for the Attorney General and provides no certainty or uniformity among the states. The Uniform Law should set out clear, uniform requirements.

**Commented [HJ32]:** This is the normal remedy for non-compliance with a consent decree or court order.

the ~~custodian's~~ controller's or processor's possession or control. Reasonable data security measures shall include administrative, technical, and physical safeguards as appropriate. Data security measures shall be evaluated as part of the data privacy assessment required under this [act]. An evaluation of the reasonableness of data security measures shall take into consideration the magnitude and likelihood of security risks and potential resulting harms, the resources available to the ~~custodian~~controller or processor, and industry practices among other ~~custodians~~ controllers or processors who are similarly situated. Reasonable security practices may be derived from best practices promulgated by professional organizations, government entities, or other specialized sources.

(b) It shall be a complete defense to liability in any enforcement action based on this Section that a controller or processor reasonably conforms to an widely adopted industry-recognized cybersecurity framework. When a final revision to an industry recognized cybersecurity framework is published, a covered entity shall reasonably conform to the revised framework not later than one year after the publication date stated in the revision.

**SECTION 11. ~~CUSTODIAN'S~~ CONTROLLER'S ~~AND~~OR PROCESSOR'S ~~DUTY~~ RESPONSIBILITY OF DATA MINIMIZATION.** A data ~~custodian~~ controller ~~or processor~~ shall not ~~collect,~~ process ~~, or retain~~ more personal data than reasonably necessary to achieve the purposes of processing. When a data controller transfers personal data to a data processor, the controller shall transfer only as much personal data as is reasonably necessary to complete the processor's processing activities. A processor shall delete, deidentify, or return personal data to the relevant controller at the agreed upon end of the provision of services or as otherwise specified by agreement.

**Commented [HJ33]:** This concept is codified in Ohio state law (OH SB 220, 2019) and is a valuable principle that incentivizes controllers and processors to adopt and follow, e.g., NIST cybersecurity frameworks, PCI-DSS principles, etc.

While the language can be massaged, we believe it is an important concept to include in the draft.

**Formatted:** Indent: First line: 0.5"

**Commented [HJ34]:** Processors collect and process what controllers instruct and authorize them to collect. Data minimization does not make sense in this context except that the processor should delete the personal information.

**SECTION 12. CONTROLLER'S ~~DUTY~~ RESPONSIBILITY OF TRANSPARENCY.**

(a) A data controller shall provide ~~data subjects~~consumers with a reasonably accessible, clear, and meaningful privacy notice which discloses the

(1) categories of personal data ~~collected or~~ processed by or on behalf of the controller;

(2) purposes for processing of personal data, either by the controller or on the controller's behalf;

(3) categories of personal data that the controller provides to processors or to any other persons;

(4) categories of processors or other persons who receive personal data from the controller;

(5) nature and purpose of any profiling of ~~data subjects~~consumers conducted using the personal data; and

(6) means by which a ~~data subject~~consumer may exercise rights provided by this [act].

(b) The notice under this section shall clearly and conspicuously designate at least two methods for a ~~data subject~~consumer to contact the data controller in order to exercise rights under this [act]. ~~At least one of these methods shall be a toll-free telephone number.~~ If the controller maintains an internet web site, at least one of these methods shall be contact through the web site.

(c) If the data controller processes personal data for targeted advertising~~-~~, or provides personal data to any processor or other person to process for targeted advertising~~-~~, the notice

**Commented [KA35]:** As stated in the comment to Section 8, ideally these two sections would be merged to have a single set of transparency requirements that a company is required to conspicuously post online/in its privacy policy. Going beyond this creates needless administrative burdens for both the AG and the controller.

**Commented [JH36]:** This would be a costly mandate and is not an absolute requirements of any state omnibus privacy law. It is particularly burdensome for small businesses, businesses that operate solely online, and processors that have a very narrow operation as a controller.

under this section shall clearly and conspicuously disclose such processing and shall provide an ~~automated internet-based mechanism~~ online location for the ~~data subject~~consumer to exercise the right to opt out of targeted advertising under this [act].

(d) The notice under this section shall be reasonably available by the data controller that collects the personal data at the time personal data is collected from a ~~data subject~~consumer.

**Commented [HJ37]:** A processor simply cannot do this.

**SECTION 13. CONTROLLER'S ~~DUTY~~ RESPONSIBILITY OF PURPOSE LIMITATION.** A controller shall not process personal data, or permit processors or other persons to process personal data, for purposes that are ~~not specified~~incompatible with the purposes in the notice to ~~data subjects~~consumers required by this [act].

**Commented [HJ38]:** This change is necessary to avoid requiring overly broad notices that will not be read.

**SECTION 14. DATA PROCESSING BY WRITTEN AGREEMENT.**

(a) Processing of personal data by a data processor ~~who is not the data controller~~ shall be governed by a written agreement between the processor and the data controller that is binding on both parties and that sets out the nature and purpose of the processing, the type of personal data subject to the processing (including the identification of any sensitive data), the duration of the processing, and the obligations and rights of both parties. The written agreement shall also provide:

(1) the data processor shall adhere to the instructions of the data controller regarding the processing of the data and shall assist the controller by adopting appropriate technological or organizational measures in fulfilling its duties under this [act].

(2) the purposes of the data processing as provided in the notice to ~~data subjects~~ consumers and that the data processor shall not process personal data for any purpose other than that stated in the agreement, except for the following purposes:~~.~~

**Commented [JH39]:** The current draft of the CCPA regs in Sec. 999.314 provide leeway for service providers to do each of the following, all of which are important for innovation and efficiency in service delivery.

(i) To process or maintain personal information on behalf of the controller that provided the personal data, or that directed the processor to collect the personal data, and in compliance with the written contract for services;

(ii) To retain and employ another processor as a subcontractor, where the subcontractor meets the requirements for a service provider under this section;

(iii) For solely internal use by the processor to build, maintain, or improve the quality of its services, provided that to the extent that the use involves building or modifying household or consumer profiles to use in providing services to a third party, or correcting or augmenting data acquired from another source, the use is consistent with any opt-out request submitted to the controller and communicated to the processor by the controller;

(iv) To detect data security incidents, or protect against fraudulent or illegal activity; or

(v) For the purposes enumerated in Section 3 of this act.

(3) The data controller has a reasonable right to request an audit of the conduct of the data processor and the data processor shall make available to the data controller all information reasonably necessary to demonstrate the processor's compliance with the requirements of this [act] and with the requirements of the contract between the controller and processor.

(4) the data processor may not transfer the personal data to another processor or to ~~any other persona~~ third party without ~~the permission of~~notice to the controller. Any such transfer must be governed by a written contract that imposes functionally ~~all~~ the same obligations on the recipient of the personal data that are imposed on the processor in the contract between the controller and the processor, regardless of whether the recipient is otherwise subject to this [act].

**Commented [HJ40]:** These audits generally need to be conducted by independent 3rd parties.

**Commented [HJ41]:** This would be a huge obstacle to efficient delivery of services in ecosystem and similar circumstances, and would give controllers the ability to leverage this power artificially to extract price or other concessions from processors. If functionally consistent obligations are imposed on subprocessors, notice to the controller is sufficient.

(5) the data controller may indemnify a data processor for liability of the data processor under this [act].

(b) The Attorney General may consider processing personal data without a written agreement consistent with this section ~~is~~ to be an unfair act and practice and subject to regulatory enforcement under Section 19. ~~A data controller who authorizes the processing of information by another without an agreement reasonably consistent with this act is subject to a private cause of action under Section 20.~~

**SECTION 15. DESIGNATION OF DATA PRIVACY OFFICER.** A data ~~custodian~~controller ~~and/or processor~~ with annual revenues in excess of $50 million shall designate an individual employee or contractor to serve as the ~~custodian~~controller's ~~and/or processor's~~ data privacy officer.

(a) A data privacy officer shall have qualifications appropriate for the supervision of the ~~custodian~~controller's ~~and/or processor's~~ responsibilities under this [act]. Minimum qualifications shall depend on the scale, complexity, and risks of the data processing activities undertaken by the ~~custodian~~controller ~~and/~~or processor.

(b) A data privacy officer shall be responsible for ~~the~~ governing the data privacy assessments required by this [act] and shall ~~sign~~ approve each data privacy assessment ~~personally~~.

(c) A data privacy officer may perform other duties for the ~~custodian~~controller ~~and/~~or ~~processor~~ ~~=~~or for other persons, provided the data privacy officer spends a reasonably sufficient amount of time directing a ~~custodian~~controller's ~~and/or processor's duties~~ responsibilities under [this law]. If a data privacy officer is not an employee of the ~~custodian~~controller ~~and/or processor~~, the ~~custodian~~controller ~~and/or processor~~ and the data privacy officer must execute a written

**Commented [HJ42]:** This invites class actions and other enforcement actions over technical contract formation quibbles and would create liability if a contract is signed a few days after authorization of a time-sensitive project.

**Commented [KA43]:** This should be applicable to large entities only; many such entities will have privacy teams, and DPA approval should lie within the department, but may be too burdensome for the DPO to personally sign each one.

agreement that clearly specifies the data privacy officer's duties. An individual may serve as a data privacy officer for more than one data ~~custodian~~controller ~~and~~or ~~processor~~.

(d) A data privacy officer may assign or delegate other persons to complete tasks under supervision, but the data privacy officer must retain authority over the completion of those tasks.

**SECTION 16. DATA PRIVACY ASSESSMENT.** A ~~custodian~~controller ~~and~~or ~~processor~~ must conduct, to the extent not previously conducted, a written data privacy assessment of each data processing activity involving sensitive personal data of more than [#] residents of this state undertaken by the ~~custodian~~controller ~~and~~or ~~processor~~, in order to evaluate all material risks, harms, and benefits of processing of those activities.

(a) A data privacy assessment shall be completed and updated about each such data processing activity ~~every two years. It shall be updated~~ any time a change in such processing activities may materially increase privacy risks to ~~data subject~~consumers.

(b) A data privacy assessment shall evaluate the:

(1) type of ~~personal~~ sensitive data being processed;

~~(2) presence of any sensitive data among the personal data being processed;~~

(3) scale of the processing activities;

(4) context in which ~~personal~~ sensitive data is collected and processed;

(5) ~~seriousness~~ potential ~~of~~ privacy risks imposed ~~on~~ for ~~data subjects~~consumers as a result of the processing;

(6) likelihood of privacy risks causing harm to ~~data subjects~~consumers as a result of the processing;

(7) benefits that may flow directly or indirectly to the ~~custodian~~controller ~~and~~or processor, ~~data subjects~~consumers, the public, or others as a result of the processing;

**Commented [HJ44]:** GDPR requires DPIAs only of processing of sensitive data. The ULC should not go beyond that expectation as there are costs to these.

**Commented [HJ45]:** Very small processing may not require a DPIA.

**Commented [HJ46]:** A material change in processing should trigger this, not the passage of 2 years.

(8) resources reasonably available to the data ~~custodian~~controller ~~and/or processor~~ for addressing privacy risks, taking account of the revenue generated by the processing; and

(9) measures the ~~custodian~~controller ~~and/or processor~~ has undertaken to mitigate any privacy risks.

(c) Privacy risks evaluated in a data privacy assessment shall encompass risks of all potential harms to ~~data subject~~consumers, including

(1) accidental disclosure, theft, or other breaches of security causing personal data to be revealed to persons without authorization;

(2) identity theft;

(3) harassment or threats against the consumer;

~~(4) unwanted profiling;~~

(5) ~~stigmatization or~~ significant reputational harm or extreme embarrassment;

~~(6) emotional harm including anxiety, embarrassment, fear, and other demonstrable mental harms;~~ and

~~(7) other foreseeable outcomes that would be highly offensive to the reasonable person.~~

(d) To satisfy its obligation under this section, a data processor may adopt data privacy assessments completed by a data controller concerning the same personal data.

(e) A data ~~custodian~~controller ~~and/or processor~~ must retain a written copy of all data privacy assessments for ~~ten~~ five years after their completion. Upon request of the [Attorney General] in connection with [an investigation], a data ~~custodian~~controller ~~and~~or processor must provide copies of all ~~current and former~~relevant data privacy assessments.

(f) Whether or not a data ~~custodian~~controller ~~and/or processor~~ has provided data privacy

**Commented [HJ47]:** This a subjective standard and is even more difficult to operationalize because of the sweeping definition of profiling.

**Commented [HJ48]:** These terms are again far too subjective to operationalize. We suggest a clearer term: "extreme embarrassment".

**Commented [HJ49]:** This is also open-ended and hard to operationalize.

assessments to the Attorney General, a data privacy assessment is confidential business information [and is not subject to public records requests or subject to compulsory civil discovery in any court].

***Legislative Note:*** *The state should include appropriate language in subsection 6(f) exempting data privacy assessments from open records requests and compulsory civil discovery requests to the maximum extent possible under state law.*

**Comment**

The primary obligation to consider and protect personal data is placed on the data controller who is the person who collects the data and directs the processing. The controller is also normally the person who deals directly with the data subject. This section requires the data controller to assess the privacy risks associated with each effort to process personal data. To encourage an open assessment of the benefits and risks, the assessment should be protected from disclosure. Otherwise the assessment will be done in a way to protect against the potential for legal liability.

While the section appears to impose the obligation of assessment on both data controllers and data processors, subjection (d) allows the processor to satisfy its obligation by obtaining the assessment of the controller. This would encourage processors to assure that their clients comply with this section and provide the processor the controller's assessment and means of mitigation of risks.

**SECTION 17. NONDISCRIMINATION.**

(a) A data controller shall not discriminate against ~~data subjects~~consumers for exercising their rights to access and copy their personal data or to request correction of inaccuracies in their personal data pursuant to section 4 by denying goods and services, charging different rates, or providing a different level of quality because the consumer requested to exercise their rights.

(b) Subject to subsection (a) of this section, a data controller may adopt and enforce as a condition for access to its goods or services that consumers permit the processing of their personal data.

**SECTION 18. WAIVERS PROHIBITED.** Any provision of a contract or agreement that purports to waive or limit rights or duties imposed by this [act] is contrary to public policy

and shall be void and unenforceable, except that a controller may indemnify a processor for liability under this [act].

**SECTION 19. REGULATORY ENFORCEMENT.**

~~(a) The [Attorney General] may adopt rules and regulations as authorized by this act. The adoption and enforcement of such rules and regulations shall be in accordance with [The Administrative Procedure Act.].~~

~~(b) The authority of the [Attorney General] to bring an action to enforce the provisions of [The Consumer Protection Act] is extended to enforce the provisions of this act.~~

~~(a) An act or practice by an entity covered by this Act shall be construed as an [unfair, deceptive, abusive] act or practice under the [consumer protection law] of this State if such act or practice:~~

~~(1) substantially fails to comply with the provisions of this Act, and/or~~

~~(2) deprives data subjects of the rights accorded by this Act.]~~

(b) The authority of the Attorney General to bring an action to enforce the provisions of the [consumer protection law] is extended to enforce the provisions of this Act.

(c) The Attorney General may bring an action to enforce the provisions of this act or [UDAP Statute] only if the controller or processor has failed to remedy an unintentional violation of this act or [UDAP statute] within 30 days after being notified in writing by the Attorney General of such unintentional violation.

~~(c) The Attorney General may adopt rules and regulations to implement the provisions of this Act. Such rules and regulations shall be adopted in accordance with the [administrative procedure act.]~~

**Commented [HJ50]:** This model law is a strict liability statute, so that a right to cure is appropriate. Indeed, the CCPA contains one. Also, as explained in the proposed exceptions, locating all data that is subject to a request can be a significant operational challenge and it is easy for businesses acting in good faith accidentally to miss stray data elements.

~~(d) In adopting rules and regulations and in bringing enforcement actions under this Act, the Attorney General shall consider the need to promote uniformity within a particular industry and among the states by:~~

~~(1) examining and, where appropriate, adopting rules and regulations consistent with the rules and regulations adopted in other states, and~~

~~(2) giving due deference to any voluntary consensus standards adopted by an industry in accordance with a process that is open, allows balanced participation by interested parties including representatives of data subjects~~consumers~~, is conducted through a fair process and provides an independent appeals process.~~

**Commented [HJ51]:** While we appreciate the intent behind this addition, "consideration" provides no guarantee of consistency, much less uniformity, across states.

***Legislative Note:*** *The state should include appropriate language cross-referencing the particular powers of the Attorney General that will be applied to enforcement of this statute and the applicable penalties.*

**Comment**

The states vary in the powers and authority granted to the Attorney General, although most states authorize the Attorney General to enforce their Consumer Protection Act. Under the Consumer Protection Act, the Attorney General can often bring a civil action to enforce the act and can seek civil penalties and injunctive relief. Such authority should be extended to enforce the provisions of this Act.

States also vary on the extent to which the Attorney General adopts rules and regulations to interpret and enforce statutory provisions. Unless prohibited by other law, the Attorney General should be specifically directed to adopt rules and regulations pursuant to this act and in accordance with the state Administrative Procedure Act.

Subsection (d) attempts to encourage uniformity among the states by requiring the Attorney General to consider actions in other states. ~~Adoption of this Act with this provision would lead naturally to the development, by state attorney general's or other groups of a set of model rules and regulations for implementing the Act.~~

The act also seeks to encourage the adoption and implementation of voluntary consensus standards by industries as long as they are adopted in an open, fair, and balanced process. The criteria are modeled on the Office of Management and Budget Circular a-119 which governs federal administrative agencies.

~~SECTION 20. PRIVATE RIGHT OF ACTION.~~

~~(A) UNLESS AUTHORIZED BY THIS SECTION, A DATA SUBJECT MAY NOT BRING A PRIVATE ACTION IN FEDERAL OR STATE COURT ALLEGING A VIOLATION OF THIS ACT.~~

~~(B)~~ ~~A DATA SUBJECT MAY BRING A PRIVATE ACTION FOR DAMAGES~~ AGAINST ~~A PERSON WHO NEGLIGENTLY OR INTENTIONALLY:~~ ~~ALLEGING THE FOLLOWING VIOLATIONS OF THE ACT:~~

~~(1) PROCESSING~~ PROCESSES ~~THE DATA SUBJECT'S PERSONAL DATA WITHOUT FILING AND PUBLISHING A PRIVACY COMMITMENT PURSUANT TO SSECTION 8~~ OF THIS ACT~~;~~

~~(2) PROCESSING~~ PROCESSES ~~THE DATA SUBJECT'S PERSONAL DATA IN A WAY THAT MATERIALLY VIOLATES THE PRIVACY COMMITMENT GOVERNING THE DATA~~ AS REQUIRED BY SECTION 8 OF THIS ACT~~;~~

~~(3) PROCESSING~~ PROCESSES ~~THE DATA SUBJECT'S DATA AFTER A FINAL DETERMINATION~~ IN A REGULATORY ACTION PURSUANT TO SECTION 19 OF THIS ACT ~~THAT THE PRIVACY COMMITMENT GOVERNING THE DATA IS AN [UNFAIR, DECEPTIVE, OR ABUSIVE PRACTICE];~~

~~(4) A DATA CONTROLLER OR DATA PROCESSOR ENGAGES~~ENGAGES ~~IN A PRACTICE WITH RESPECT TO THE DATA SUBJECT'S DATA AFTER A FINAL DECISION IN A REGULATORY ENFORCEMENT ACTION FINDING THAT THE PRACTICE IS [UNFAIR, DECEPTIVE, OR ABUSIVE].~~

**Commented [HJ52]:** The rights in this law are far too operationally complex to make a private right of action fair or appropriate. For this reason, the California legislature has twice rejected proposals to enforce CCPA privacy rights through a private right of action. The ULC would be far ahead of any state law in doing so.

**Formatted:** Heading 1, Line spacing: single, Widow/Orphan control

~~(5) A VIOLATION OF SECTION 14 OF THIS ACT~~PROCESSES A DATA SUBJECT'S DATA WITHOUT AN AGREEMENT PURSUANT TO SECTION 14 OF THIS ACT.

~~(B) DAMAGES AVAILABLE TO A PERSON IN A SUIT UNDER THIS SECTION SHALL BE ACTUAL DAMAGES OR DAMAGES OF [$100], WHICHEVER IS GREATER.~~

~~(C) EVIDENCE ABOUT THE DEVELOPMENT OR RESULTS OF A DATA PRIVACY ASSESSMENT IS NOT SUBJECT TO COMPULSORY DISCOVERY IN A CIVIL SUIT BROUGHT UNDER THIS [ACT], AND SHALL BE TREATED BY THE COURT IN THE SAME MANNER AS A CONFIDENTIAL OFFER OF SETTLEMENT, UNLESS A DATA CUSTODIAN~~CONTROLLER ~~AND~~OR PROCESSOR ~~VOLUNTARILY INTRODUCES EVIDENCE RELATED TO A DATA PRIVACY ASSESSMENT. IF A DATA CUSTODIAN~~CONTROLLER ~~AND~~OR PROCESSOR ~~VOLUNTARILY INTRODUCES EVIDENCE RELATED TO A DATA PRIVACY ASSESSMENT, ADMISSIBILITY AND DISCOVERABILITY OF EVIDENCE RELATED TO THAT DATA PRIVACY ASSESSMENT SHALL BE HANDLED IN ACCORDANCE WITH THE COURT'S ORDINARY RULES OF EVIDENCE.~~

**Comment**

~~This section provides a limited private cause of action to persons injured by specified violations of the Act. Whether or not to authorize a private cause of action has been a matter of considerable controversy.~~ The substantive provisions of any data privacy act must be broad in order to encompass the wide variety of data uses and industries to which it applies. Such provisions make it difficult for data ~~custodian~~controller ~~and~~or processors to assure in advance that it has met all technical requirements and provides plaintiffs and their lawyers considerable leverage to force settlements and large judgments. ~~On the other hand, leaving enforcement solely to a public agency, particularly a State Attorney General's office, is subject to the resource allocation and priorities of each office.~~

~~Section 20 attempts to respond to both concerns. Private causes of action are limited to circumstances in which the obligation on a data custodiancontroller andor processors is either clear or can be tailored by the custodiancontroller and or processor to create a safe harbor. Conduct is only actionable on proof of negligence or intentional conduct. Of particular importance is section 8 which requires a data controller to publish and file with the Attorney General a "privacy commitment" a document that would specify the manner in which data subject consumers may exercise their rights under the act and the method in which the controller will respond to the assertion of those rights. This would allow an entity to adopt codes of conductbest practices or voluntary consensus standards particular to its industry and the nature of its data processing.~~

The privacy commitment would be subject to review by the Attorney General and through regulatory enforcement could be rejected. However, as long as the commitment was enforce, compliance would serve as a safe harbor from private actions. Violations of the commitment or failure to publish a commitment would be subject to a private cause of action.

~~The section also authorizes a private cause of action where a data controller fails to establish a written agreement for the processing of personal data.~~ Most of the obligations under the Act are imposed on the controller as the entity that is in a direct relationship with the ~~data subject~~consumer. However, it is essential the controller, through contract, impose the same obligations on a data processor.

**SECTION 21. UNIFORMITY OF APPLICATION AND CONSTRUCTION.** In applying and construing this uniform act, consideration must be given to the need to promote uniformity of the law with respect to its subject matter among states that enact it.

**SECTION 22. PREEMPTION.** This [act] supersedes and preempts laws, ordinances, regulations, or the equivalent adopted by any local entity regarding the processing of personal data by covered entities to the extent that they apply to the activities regulated by this state.

**Commented [HJ53]:** Local preemption is critical to uniformity and is in the CCPA.

~~**SECTION 22. RELATION TO ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT.** This [act] modifies, limits, and supersedes the federal Electronic Signatures in Global and National Commerce Act, 15 U.S.C. Section 7001, et seq., but does not modify, limit, or supersede Section 101(c) of that act, 15 U.S.C. Section 7001(c), or authorize electronic delivery of any of the notices described in Section 103(b) of that act, 15 U.S.C. Section 7003(b).~~

**Commented [HJ54]:** No state privacy law purports to do this and it is far from clear that trying to evade E-SIGN would serve any significant purpose or would even be effective given that E-SIGN broadly preempts state law.

**SECTION 23. SEVERABILITY.** If any provision of this [act] or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this [act] which can be given effect without the invalid provision or application, and to this end the provisions of this [act] are severable.

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

**SECTION 24. EFFECTIVE DATE.** This [act] takes effect one year ~~[180 days]~~ after the date of enactment.

**Commented [HJ55]:** In several ways, these requirements go beyond CCPA. They are intensely operational, would go into effect during or shortly after a deep recession and require more time to implement.

**Commented [HJ56]:** AG rulemaking would require the implementation clock to start running after the rulemaking was complete, not the date of enactment.