

THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

No. 1201 Session of 2023

INTRODUCED BY NEILSON, CIRESI, McNEILL, KHAN, SANCHEZ, KINSEY, CEPEDA-FREYTIZ, PARKER, HILL-EVANS, GALLOWAY, GREEN, WAXMAN AND OTTEN, MAY 19, 2023

AS REPORTED FROM COMMITTEE ON COMMERCE, HOUSE OF REPRESENTATIVES, AS AMENDED, NOVEMBER 15, 2023

AN ACT

1 Providing for consumer data privacy, for duties of controllers
2 and for duties of processors; and imposing penalties.

3 The General Assembly of the Commonwealth of Pennsylvania
4 hereby enacts as follows:

5 Section 1. Short title.

6 This act shall be known and may be cited as the Consumer Data
7 Privacy Act.

8 Section 2. Definitions.

9 The following words and phrases when used in this act shall
10 have the meanings given to them in this section unless the
11 context clearly indicates otherwise:

12 "AFFILIATE." A LEGAL ENTITY THAT SHARES COMMON BRANDING WITH <--
13 ANOTHER LEGAL ENTITY OR CONTROLS, IS CONTROLLED BY OR IS UNDER
14 COMMON CONTROL WITH ANOTHER LEGAL ENTITY.

15 "Biometric data." Data generated by automatic measurements
16 of an individual's biological characteristics, including
17 fingerprints, voiceprints, eye retinas, irises or other unique

1 biological patterns or characteristics that are used to identify
2 a specific individual. The term does not include a digital or
3 physical photograph, an audio or video recording or any data
4 generated from a digital or physical photograph or an audio or
5 video recording, unless the data is generated to identify a <--
6 specific individual. RECORDING. THE TERM DOES NOT INCLUDE <--
7 INFORMATION CAPTURED AND CONVERTED TO A MATHEMATICAL
8 REPRESENTATION, INCLUDING A NUMERIC STRING OR SIMILAR METHOD
9 THAT CANNOT BE USED TO RECREATE THE DATA CAPTURED OR CONVERTED
10 TO CREATE THE MATHEMATICAL REPRESENTATION.

11 "Business associate." As defined in 45 CFR 160.103 (relating
12 to definitions)

13 "Child." As defined in 15 U.S.C. § 6501 (relating to
14 definitions).

15 "Common branding." A shared name, servicemark or trademark.

16 "Consent." A clear affirmative act signifying a consumer's
17 freely given, specific, informed and unambiguous agreement to
18 allow the processing of personal data relating to the consumer.
19 The term includes a written statement, including by electronic
20 means, or any other unambiguous affirmative action specified in
21 this definition. The term does not include acceptance of general
22 or broad terms of use or a similar document that contains
23 descriptions of personal data processing along with other
24 unrelated information, hovering over, muting, pausing or closing
25 a given piece of content or an agreement obtained through the
26 use of dark patterns.

27 "Consumer." An individual who is a resident of this
28 Commonwealth. The term does not include an individual acting in
29 a commercial or employment context or as an employee, owner,
30 director, officer or contractor of a company, partnership, sole

1 proprietorship, nonprofit or government agency whose
2 communications or transactions with a controller occur solely
3 within the context of that individual's role with the company,
4 partnership, sole proprietorship, nonprofit or government
5 agency.

6 "Control." Any of the following:

7 (1) Ownership of or the power to vote on more than 50%
8 of the outstanding shares of any class of voting security of
9 a controller.

10 (2) Control in any manner over the election of a
11 majority of the directors or over the individuals exercising
12 similar functions.

13 (3) The power to exercise a controlling influence over
14 the management of a company.

15 "Controller." As follows:

16 (1) A sole proprietorship, partnership, limited
17 liability company, corporation, association or other legal
18 entity that meets all of the following criteria:

19 (i) Is organized or operated for the profit or
20 financial benefit of its shareholders or other owners.

21 ~~(ii) Collects consumers' personal information or on~~ <--
22 ~~behalf of which consumers' personal information is~~
23 ~~collected and that, alone or jointly with others,~~
24 ~~determines the purposes and means of the processing of~~
25 ~~consumers' personal information.~~ ALONE OR JOINTLY WITH <--
26 OTHERS, DETERMINES THE PURPOSES AND MEANS OF THE
27 PROCESSING OF CONSUMERS' PERSONAL INFORMATION.

28 (iii) Does business in this Commonwealth.

29 (iv) Satisfies any of the following thresholds:

30 (A) Has annual gross revenues in excess of

1 \$10,000,000.

2 (B) Alone or in combination, annually buys or
3 receives, sells or shares for commercial purposes,
4 alone or in combination, the personal information of
5 at least 50,000 consumers, households or devices.

6 (C) Derives at least 50% of annual revenues from
7 selling consumers' personal information.

8 (2) An entity that controls a sole proprietorship,
9 partnership, limited liability company, corporation,
10 association or other legal entity under paragraph (1) and
11 shares common branding with the sole proprietorship,
12 partnership, limited liability company, corporation,
13 association or other legal entity.

14 "Covered entity." As defined in 45 CFR 160.103.

15 "Dark pattern." A user interface designed or manipulated
16 with the substantial effect of subverting or impairing user
17 autonomy, decision making or choice, including a practice the
18 Federal Trade Commission refers to as a dark pattern.

19 "Decisions that produce legal or similarly significant
20 effects concerning the consumer." Decisions made by a
21 controller that result in the provision or denial by the
22 controller of financial or lending services, housing, insurance,
23 education enrollment or opportunity, criminal justice,
24 employment opportunities, health care services or access to
25 essential goods or services.

26 "De-identified data." Data that cannot reasonably be used to
27 infer information about, or otherwise be linked to, an
28 identified or identifiable individual or a device linked to the
29 individual, if the controller that possesses the data complies
30 with the following criteria:

1 (1) Takes reasonable measures to ensure that the data
2 cannot be associated with an individual.

3 (2) Publicly commits to process the data only in a de-
4 identified fashion and not attempt to re-identify the data.

5 (3) Contractually obligates a recipient of the data to
6 satisfy the criteria specified under paragraphs (1) and (2).

7 "HIPAA." The Health Insurance Portability and Accountability
8 Act of 1996 (Public Law 104-191, 110 Stat. 1936).

9 "Identified or identifiable individual." An individual who
10 can be readily identified, directly or indirectly.

11 "Institution of higher education." As defined in section
12 118(c) of the act of March 10, 1949 (P.L.30, No.14), known as
13 the Public School Code of 1949.

14 "Nonprofit organization." An organization that is exempt
15 from taxation under 26 U.S.C. § 501(c) (3), (4), (6) or (12)
16 (relating to exemption from tax on corporations, certain trusts,
17 etc.).

18 "Personal data." As follows:

19 ~~(1) Information that identifies, relates to, describes, <--~~
20 ~~is capable of being associated with or could reasonably be~~
21 ~~linked, directly or indirectly, with a particular consumer or~~
22 ~~household, including any of the following:~~

23 ~~(i) An identifier, including a real name, alias,~~
24 ~~postal address, unique personal identifier, online~~
25 ~~identifier, including an Internet website protocol~~
26 ~~address, email address or account name, Social Security~~
27 ~~number, driver's license number, passport number or other~~
28 ~~similar identifiers.~~

29 ~~(ii) Characteristics of protected classifications~~
30 ~~under Federal or State law.~~

1 ~~(iii) Commercial information, including records of~~
2 ~~personal property, products or services purchased,~~
3 ~~obtained or considered or other purchasing or consuming~~
4 ~~histories or tendencies.~~

5 ~~(iv) Biometric data.~~

6 ~~(v) Internet or other electronic network activity~~
7 ~~information, including browser history, search history~~
8 ~~and information regarding a consumer's interaction with~~
9 ~~an Internet website, application or advertisement.~~

10 ~~(vi) Precise geolocation data.~~

11 ~~(vii) Audio, electronic, visual, thermal, olfactory~~
12 ~~or similar information.~~

13 ~~(viii) Professional or employment related~~
14 ~~information.~~

15 ~~(ix) Education information that is not publicly~~
16 ~~available personally identifiable information under 20~~
17 ~~U.S.C. § 1232g (relating to family educational and~~
18 ~~privacy rights).~~

19 ~~(x) An inference drawn from any of the information~~
20 ~~identified under this definition to create a profile~~
21 ~~about a consumer reflecting the consumer's preferences,~~
22 ~~characteristics, psychological trends, predispositions,~~
23 ~~behaviors, attitudes, intelligence, abilities or~~
24 ~~aptitudes.~~

25 ~~(2) The term does not include publicly available~~
26 ~~information.~~

27 (1) ANY INFORMATION THAT IS LINKED OR REASONABLY
28 LINKABLE TO AN IDENTIFIED OR IDENTIFIABLE INDIVIDUAL.

<--

29 (2) THE TERM DOES NOT INCLUDE PUBLICLY AVAILABLE
30 INFORMATION, DE-IDENTIFIED DATA OR BIOMETRIC DATA CAPTURED

1 AND CONVERTED TO A MATHEMATICAL REPRESENTATION.

2 "Precise geolocation data." Information derived from
3 technology, including global positioning system level latitude
4 and longitude coordinates or other mechanisms, that directly
5 identify the specific location of an individual with precision
6 and accuracy within a radius of 1,750 feet. The term does not
7 include the content of communications, or any data generated by <--
8 or connected to advanced utility metering infrastructure systems
9 or equipment for use by a utility.

10 "Process" or "processing." Any operation or set of
11 operations performed, whether by manual or automated means, on
12 personal data or on sets of personal data, including the
13 collection, use, storage, disclosure, analysis, deletion or
14 modification of personal data.

15 "Processing activities that present a heightened risk of harm
16 to a consumer." The term includes any of the following:

17 (1) The processing of personal data for the purpose of
18 targeted advertising.

19 (2) The sale of personal data.

20 (3) The processing of personal data for the purpose of
21 profiling if the profiling presents a reasonably foreseeable
22 risk of any of the following:

23 (i) Unfair or deceptive treatment of, or an unlawful
24 disparate impact on, a consumer.

25 (ii) Financial, physical or reputational injury to a
26 consumer.

27 (iii) A physical or other intrusion upon the
28 solitude or seclusion of a consumer or the private
29 affairs or concerns of a consumer where the intrusion
30 would be offensive to a reasonable person.

1 (iv) Any other substantial injury to a consumer.

2 (4) The processing of sensitive data.

3 "Processor." An individual who, or legal entity that,
4 processes personal data on behalf of a controller.

5 "Profiling." Any form of automated processing performed on
6 personal data to evaluate, analyze or predict personal aspects
7 related to an identified or identifiable individual's economic
8 situation, health, personal preferences, interests, reliability,
9 behavior, location or movements.

10 "Protected health information." As defined in 45 CFR
11 160.103.

12 "Pseudonymous data." Personal data that cannot be attributed
13 to a specific individual without the use of additional
14 information if the additional information is kept separately and
15 is subject to appropriate technical and organizational measures
16 to ensure that the personal data is not attributed to an
17 identified or identifiable individual.

18 "Publicly available information." ~~As follows:~~ <--

19 ~~(1) Information that is lawfully made available from~~
20 ~~Federal, State or local government records as restricted by~~
21 ~~any conditions associated with the information.~~

22 ~~(2) The term does not include biometric data collected~~
23 ~~by a controller about a consumer without the consumer's~~
24 ~~knowledge or consumer information that is de identified or~~
25 ~~aggregate consumer information.~~

26 ~~(3) For the purpose of this definition, information~~
27 ~~shall not be considered publicly available if the data is~~
28 ~~used for a purpose that is not compatible with the purpose~~
29 ~~for which the data is maintained and made available in~~
30 ~~Federal, State or local government records or for which the~~

1 ~~data is publicly maintained.~~ INFORMATION THAT:

2 (1) IS LAWFULLY AVAILABLE THROUGH FEDERAL, STATE OR
3 MUNICIPAL RECORDS OR WIDELY DISTRIBUTED MEDIA; OR

4 (2) A CONTROLLER HAS A REASONABLE BASIS TO BELIEVE A
5 CONSUMER HAS LAWFULLY MADE AVAILABLE TO THE GENERAL PUBLIC.

6 "Sale of personal data." The exchange of personal data for
7 monetary or other valuable consideration by a controller to a
8 third party. The term does not include any of the following:

9 (1) The disclosure of personal data to a processor that
10 processes the personal data on behalf of the controller.

11 (2) The disclosure of personal data to a third party for
12 the purpose of providing a product or service requested by a
13 consumer.

14 (3) The disclosure or transfer of personal data to an
15 affiliate of the controller.

16 (4) The disclosure of personal data when a consumer
17 directs the controller to disclose the personal data or
18 intentionally uses the controller to interact with a third
19 party.

20 (5) The disclosure of personal data that a consumer:

21 (i) intentionally made available to the general
22 public via a channel of mass media; and

23 (ii) did not restrict to a specific audience.

24 (6) The disclosure or transfer of personal data to a
25 third party as an asset that is part of a merger,
26 acquisition, bankruptcy or other transaction or a proposed
27 merger, acquisition, bankruptcy or other transaction, in
28 which the third party assumes control of all or part of the
29 controller's assets.

30 "Sensitive data." Personal data that includes data revealing

1 any of the following:

2 (1) A racial or ethnic origin.

3 (2) Religious beliefs.

4 (3) Mental or physical health condition or diagnosis.

5 (4) Sex life or sexual orientation.

6 (5) Citizenship or immigration status.

7 (6) The processing of genetic or biometric data for the
8 purpose of uniquely identifying an individual.

9 (7) Personal data collected from a known child.

10 (8) Precise geolocation data.

11 "Targeted advertising." Displaying advertisements to a
12 consumer if the advertisement is selected based on personal data
13 obtained or inferred from the consumer's activities over time
14 and across nonaffiliated Internet websites or online
15 applications to predict the consumer's preferences or interests.
16 The term does not include any of the following:

17 (1) Advertisements based on activities within a
18 controller's own Internet websites or online applications.

19 (2) Advertisements based on the context of a consumer's
20 current search query, visit to an Internet website or online
21 application.

22 (3) Advertisements directed to a consumer in response to
23 the consumer's request for information or feedback.

24 (4) Processing personal data solely to measure or report
25 advertising frequency, performance or reach.

26 "Third party." An individual or legal entity, including a
27 public authority, agency or body, other than a consumer,
28 controller or processor or an affiliate of the processor or the
29 controller.

30 "TRADE SECRET." AS DEFINED IN 12 PA.C.S. § 5302 (RELATING TO <--

1 DEFINITIONS).

2 Section 3. Consumer data privacy.

3 (a) Rights of consumers.--A consumer shall have the right to
4 do the following:

5 (1) Confirm whether or not a controller is processing or
6 accessing the consumer's personal data, UNLESS THE <--
7 CONFIRMATION OR ACCESS WOULD REQUIRE THE CONTROLLER TO REVEAL
8 A TRADE SECRET.

9 (2) Correct inaccuracies in the consumer's personal
10 data, taking into account the nature of the personal data and
11 the purposes of the processing of the consumer's personal
12 data.

13 (3) Delete personal data provided by or obtained about
14 the consumer.

15 (4) Obtain a copy of the consumer's personal data
16 processed by a controller in a portable and, to the extent
17 technically feasible, readily usable format that allows the
18 consumer to transmit the data to another controller without
19 hindrance, where the processing is carried out by automated
20 means IN A MANNER THAT WOULD DISCLOSE THE CONTROLLER'S TRADE <--
21 SECRETS.

22 (5) Opt out of the processing of the consumer's personal
23 data for the purpose of any of the following:

24 (i) Targeted advertising.

25 (ii) The sale of personal data, except as provided
26 under section 5(b).

27 (iii) Profiling in furtherance of solely automated
28 decisions that produce legal or similarly significant
29 effects concerning the consumer.

30 (b) Exercise of rights.--A consumer may exercise the rights

1 under subsection (a) by a secure and reliable means established
2 by a controller and described to the consumer in the
3 controller's privacy notice. A consumer may designate an
4 authorized agent in accordance with section 4 to exercise the
5 consumer's right under subsection (a) (5) to opt out of the
6 processing of the consumer's personal data on behalf of the
7 consumer. For processing personal data of a known child, the
8 parent or legal guardian may exercise the consumer's rights
9 under subsection (a) on the child's behalf. For processing
10 personal data concerning a consumer subject to a guardianship,
11 conservatorship or other protective arrangement, the guardian or
12 the conservator of the consumer may exercise the consumer's
13 rights under subsection (a) on the consumer's behalf.

14 (c) Compliance.--Except as otherwise provided in this act, a
15 controller shall comply with a request by a consumer to exercise
16 the consumer's rights under subsection (a) as follows:

17 (1) The controller shall respond to the consumer without
18 undue delay, but no later than 45 days after receipt of the
19 request. The controller may extend the response period under
20 this paragraph by an additional 45 days when reasonably
21 necessary, considering the complexity and number of the
22 consumer's requests, if the controller informs the consumer
23 of the extension within the initial 45-day response period
24 and the reason for the extension.

25 (2) If the controller declines to take action regarding
26 the consumer's request, the controller shall inform the
27 consumer without undue delay, but no later than 45 days after
28 receipt of the request, of the justification for declining to
29 take action and instructions for how to appeal the decision.

30 (3) Information provided in response to consumer

1 requests shall be provided by the controller, free of charge,
2 once per consumer during a 12-month period. If a request from
3 a consumer is manifestly unfounded, excessive or repetitive,
4 the controller may charge the consumer a reasonable fee to
5 cover the administrative costs of complying with the request
6 or decline to act on the request. The controller bears the
7 burden of demonstrating the manifestly unfounded, excessive
8 or repetitive nature of the request.

9 (4) If a controller is unable to authenticate a request
10 to exercise a right afforded under subsection (a) (1), (2),
11 (3) or (4) using commercially reasonable efforts, the
12 controller shall not be required to comply with a request
13 under this subsection and shall provide notice to the
14 consumer that the controller is unable to authenticate the
15 request to exercise the right until the consumer provides
16 additional information reasonably necessary to authenticate
17 the consumer and the consumer's request to exercise the
18 right. A controller shall not be required to authenticate an
19 opt-out request under subsection (a) (5), but the controller
20 may deny an opt-out request if the controller has a good
21 faith, reasonable and documented belief that the request is
22 fraudulent. If a controller denies an opt-out request under
23 subsection (a) (5) because the controller believes the request
24 is fraudulent, the controller shall send a notice to the
25 person who made the request disclosing that the controller
26 believes the request is fraudulent, why the controller
27 believes the request is fraudulent and that the controller
28 will not comply with the request.

29 (5) A controller that has obtained personal data about a
30 consumer from a source other than the consumer shall be

1 deemed in compliance with a consumer's request to delete the
2 personal data in accordance with subsection (a) (3) by
3 retaining a record of the deletion request and the minimum
4 data necessary for the purpose of ensuring that the
5 consumer's personal data remains deleted from the
6 controller's records and not using such retained data for any
7 other purpose in accordance with the provisions of this act
8 OR OPTING THE CONSUMER OUT OF THE PROCESSING OF THE DATA FOR <--
9 ANY PURPOSE EXCEPT FOR THOSE EXEMPTED UNDER SECTION 11(A) (3) .

10 (d) Appeals.--A controller shall establish a process for a
11 consumer to appeal the controller's refusal to take action on a
12 request by a consumer to exercise the consumer's rights under
13 subsection (a) within a reasonable period of time after the
14 consumer's receipt of the decision under subsection (c) (2) . The
15 appeal process shall be conspicuously available and similar to
16 the process for submitting requests to initiate an action under
17 subsection (b) . No later than 60 days after receipt of an
18 appeal, the controller shall inform the consumer in writing of
19 an action taken or not taken in response to the appeal,
20 including a written explanation of the reason for the decision.
21 If the appeal is denied, the controller shall also provide the
22 consumer with an online mechanism, if available, or other method
23 through which the consumer may contact the Attorney General to
24 submit a complaint.

25 Section 4. Designation of authorized agent.

26 A consumer may designate another person to serve as the
27 consumer's authorized agent and act on the consumer's behalf to
28 opt out of the processing of the consumer's personal data for
29 the purposes specified under section 3(a) (5) . A controller shall
30 comply with an opt-out request received from an authorized agent

1 under section 3(a)(5) if the controller is able to verify, with
2 commercially reasonable effort, the identity of the consumer and
3 the authorized agent's authority to act on the consumer's
4 behalf.

5 Section 5. Duties of controllers.

6 (a) Duties.--A controller shall have all of the following
7 duties:

8 (1) Limit the collection of personal data to what is
9 adequate, relevant and reasonably necessary in relation to
10 the purposes for which the data is processed, as disclosed to
11 the consumer.

12 (2) Except as otherwise provided in this act, refrain
13 from processing personal data for purposes that are neither
14 reasonably necessary to, nor compatible with, the disclosed
15 purposes for which the personal data is processed, as
16 disclosed to the consumer, unless the controller obtains the
17 consumer's consent.

18 (3) ~~Establish, implement and maintain reasonable~~ <--
19 ~~administrative, technical and physical data security~~
20 ~~practices to protect the confidentiality, integrity and~~
21 ~~accessibility of personal data appropriate to the volume and~~
22 ~~nature of the personal data at issue.~~ PROCESS PERSONAL DATA <--
23 IN A MANNER THAT ENSURES REASONABLE AND APPROPRIATE
24 ADMINISTRATIVE, TECHNICAL, ORGANIZATIONAL AND PHYSICAL
25 SAFEGUARDS OF PERSONAL DATA COLLECTED, STORED AND PROCESSED.

26 (4) Refrain from processing sensitive data concerning a
27 consumer without obtaining the consumer's consent or, in the
28 case of the processing of sensitive data concerning a known
29 child, without processing the data, in accordance with 15
30 U.S.C. Ch. 91 (relating to children's online privacy

1 protection).

2 (5) Refrain from processing personal data in violation
3 of a Federal or State law that prohibits unlawful
4 discrimination against a consumer.

5 (6) Provide an effective mechanism for a consumer to
6 revoke the consumer's consent that is at least as easy as the
7 mechanism by which the consumer provided the consumer's
8 consent and, upon revocation of the consent, cease to process
9 the data as soon as practicable, but no later than 15 days
10 after the receipt of the request.

11 (7) Refrain from processing the personal data of a
12 consumer for the purpose of targeted advertising or selling
13 the consumer's personal data without the consumer's consent
14 under circumstances where the controller has actual knowledge
15 and willfully disregards that the consumer is younger than 16
16 years of age.

17 (8) Refrain from discriminating against a consumer for
18 exercising any of the consumer rights under section 3(a),
19 including denying goods or services, charging different
20 prices or rates for goods or services or providing a
21 different level of quality of goods or services to the
22 consumer.

23 (b) Construction.--Nothing in subsection (a) shall be
24 construed to require a controller to provide a product or
25 service that requires the personal data of a consumer that the
26 controller does not collect or maintain nor prohibit a
27 controller from offering a different price, rate, level, quality
28 or selection of goods or services to a consumer, including
29 offering goods or services for no fee, if the offering is in
30 connection with a consumer's voluntary participation in a bona

1 fide loyalty, rewards, premium features, discounts or club card
2 program.

3 (c) Privacy notice.--A controller shall provide a consumer
4 with a reasonably accessible, clear and meaningful privacy
5 notice that includes all of the following:

6 (1) The categories of personal data processed by the
7 controller.

8 (2) The purpose for processing personal data.

9 (3) How the consumer may exercise the consumer's rights,
10 including how the consumer may appeal the controller's
11 decision with regard to the consumer's request under section
12 3(d).

13 (4) The categories of personal data that the controller
14 shares with each third party.

15 (5) The categories of each third party with which the
16 controller shares personal data.

17 (6) An active email address or other online mechanism
18 that the consumer may use to contact the controller.

19 (d) Disclosures.--If a controller sells personal data to a
20 third party or processes personal data for targeted advertising,
21 the controller shall clearly and conspicuously disclose the sale
22 or processing and the manner in which a consumer may exercise
23 the right to opt out of the sale or processing.

24 (e) Means to exercise rights.--

25 (1) A controller shall establish and describe in the
26 privacy notice under subsection (c) a secure and reliable
27 means for consumers to submit a request to exercise the
28 consumer's rights under section 3(a). The secure and reliable
29 means under this paragraph shall take into account the manner
30 in which a consumer normally interacts with the controller,

1 the need for secure and reliable communication for the
2 request and the ability of the controller to verify the
3 identity of the consumer making the request. A controller may
4 not require a consumer to create a new account in order to
5 exercise the consumer's rights under section 3(a), but may
6 require the consumer to use an existing account. The secure
7 and reliable means shall include all of the following:

8 (i) Providing a clear and conspicuous link on the
9 controller's Internet website to an Internet web page
10 that enables a consumer, or an agent of the consumer, to
11 opt out of the targeted advertising or sale of the
12 consumer's personal data under section 3(a)(5).

13 (ii) No later than January 1, 2026, allowing a
14 consumer to opt out of the processing of the consumer's
15 personal data for the purpose of targeted advertising or
16 the sale of the consumer's personal data under section
17 3(a)(5) through an opt-out preference signal sent, with
18 the consumer's consent, by a platform, technology or
19 mechanism to the controller indicating the consumer's
20 intent to opt out of the processing or sale. The
21 platform, technology or mechanism shall comply with all
22 of the following criteria:

23 (A) Not unfairly disadvantage another
24 controller.

25 (B) Not make use of a default setting, but
26 instead require the consumer to make an affirmative,
27 freely given and unambiguous choice to opt out of the
28 processing or sale of the consumer's personal data.

29 (C) Be consumer friendly and easy to use by the
30 average consumer.

1 (D) Be as consistent as possible with any other
2 similar platform, technology or mechanism required by
3 a Federal or State law or regulation.

4 (E) Enable the controller to accurately
5 determine whether the consumer is a resident of this
6 Commonwealth and whether the consumer has made a
7 legitimate request to opt out of processing or sale
8 of the consumer's personal data.

9 (F) BE IN COMPLIANCE WITH THIS SECTION. A <--
10 CONTROLLER THAT RECOGNIZES SIGNALS APPROVED BY OTHER
11 STATES SHALL BE CONSIDERED IN COMPLIANCE WITH THIS
12 SECTION.

13 (iii) If a consumer's decision to opt out of the
14 processing of the consumer's personal data for the
15 purpose of targeted advertising or the sale of the
16 consumer's personal data under section 3(a)(5) through an
17 opt-out preference signal sent under subparagraph (ii)
18 conflicts with the consumer's existing controller-
19 specific privacy setting or voluntary participation in a
20 controller's bona fide loyalty, rewards, premium
21 features, discounts or club card program, the controller
22 shall comply with the consumer's opt-out preference
23 signal, but may notify the consumer of the conflict and
24 provide to the consumer the choice to confirm the
25 controller-specific privacy setting or participation in
26 the program.

27 (2) If a controller responds to a consumer's opt-out
28 request under paragraph (1)(i) by informing the consumer of a
29 charge for the use of a product or service, the controller
30 shall present the terms of a bona fide loyalty, rewards,

1 premium features, discounts or club card program for the
2 retention, use, sale or sharing of the consumer's personal
3 data.

4 Section 6. Duties of processors.

5 (a) Assistance.--A processor shall adhere to the
6 instructions of a controller and shall assist the controller in
7 complying with the controller's duties under this act. The
8 assistance shall include all of the following:

9 (1) Taking into account the nature of processing and the
10 information available to the processor, by appropriate
11 technical and organizational measures, insofar as is
12 reasonably practicable, to fulfill the controller's duty to
13 comply with a request by a consumer to exercise the
14 consumer's rights under section 3(a).

15 (2) Taking into account the nature of processing and the
16 information available to the processor, by assisting the
17 controller in meeting the controller's duties in relation to
18 the security of processing the personal data and in relation
19 to the notification of a breach of security of the system of
20 the processor.

21 (3) Providing necessary information to enable the
22 controller to conduct and document data protection
23 assessments.

24 (b) Contracts.--A contract between a controller and a
25 processor shall govern the processor's data processing
26 procedures with respect to processing performed on behalf of the
27 controller. The contract shall be binding and clearly state the
28 instructions for processing data, the nature and purpose of
29 processing, the type of data subject to processing, the duration
30 of processing and the rights and obligations of both parties.

1 The contract shall also require that the processor comply with
2 all of the following:

3 (1) Ensure that each person processing personal data is
4 subject to a duty of confidentiality with respect to the
5 data.

6 (2) At the controller's direction, delete or return all
7 personal data to the controller as requested at the end of
8 the provision of services, unless retention of the personal
9 data is required by Federal or State law.

10 (3) Upon the reasonable request of the controller, make
11 available to the controller all information in the
12 processor's possession necessary to demonstrate the
13 processor's compliance with the provisions of this act.

14 (4) After providing the controller with an opportunity
15 to object, engage a subcontractor pursuant to a written
16 contract that requires the subcontractor to meet the
17 obligations of the processor with respect to the personal
18 data.

19 (5) Allow and cooperate with a reasonable assessment by
20 the controller or the controller's designated assessor, or
21 arrange for a qualified and independent assessor to conduct
22 an assessment of the processor's policies and technical and
23 organizational measures in support of the requirements under
24 this act, using an appropriate and accepted control standard
25 or framework and assessment procedure for the assessment. The
26 processor shall provide a report of the assessment to the
27 controller upon request.

28 (c) Construction.--Nothing in this section shall be
29 construed to relieve a controller or processor from the
30 liabilities imposed on the controller or processor by virtue of

1 the role of the controller or processor in the processing
2 relationship specified under this act.

3 (d) Acting as controller or processor.--A determination of
4 whether a person is acting as a controller or processor with
5 respect to a specific processing of data shall be a fact-based
6 determination that depends upon the context in which personal
7 data is to be processed. The following shall apply:

8 (1) A person who is not limited in the person's
9 processing of personal data pursuant to a controller's
10 instructions or who fails to adhere to the instructions shall
11 be a controller and not a processor with respect to a
12 specific processing of data.

13 (2) A processor who continues to adhere to a
14 controller's instructions with respect to a specific
15 processing of personal data shall remain a processor.

16 (3) If a processor begins, alone or jointly with others,
17 determining the purposes and means of the processing of
18 personal data, the processor shall be a controller with
19 respect to the processing and may be subject to an
20 enforcement action under section 10.

21 Section 7. Data protection assessment.

22 (a) Assessment.--A controller shall conduct and document a
23 data protection assessment for each of the controller's
24 processing activities that present a heightened risk of harm to
25 a consumer.

26 (b) Benefits and risks.--In conducting a data protection
27 assessment under subsection (a), a controller shall identify and
28 weigh the benefits that may flow, directly and indirectly, from
29 the processing to the controller, the consumer, other
30 stakeholders and the public against the potential risks to the

1 consumer's rights under section 3(a) associated with the
2 processing, as mitigated by safeguards that can be employed by
3 the controller to reduce the risks. The controller shall factor
4 all of the following into the data protection assessment:

- 5 (1) The use of de-identified data.
- 6 (2) The reasonable expectations of the consumer.
- 7 (3) The context of the processing and the relationship
8 between the controller and the consumer whose personal data
9 will be processed.

10 (c) Availability of assessments.--The Attorney General may
11 require a controller to disclose a data protection assessment
12 under subsection (a) that is relevant to an investigation
13 conducted by the Attorney General, and the controller shall make
14 the data protection assessment available to the Attorney
15 General. The Attorney General may evaluate a data protection
16 assessment for compliance with the provisions of this act. A
17 data protection assessment shall be confidential and exempt from
18 disclosure under 5 U.S.C. § 552 (relating to public information;
19 agency rules, opinions, orders, records, and proceedings) and
20 the act of February 14, 2008 (P.L.6, No.3), known as the Right-
21 to-Know Law. To the extent that information contained in a data
22 protection assessment disclosed to the Attorney General under
23 this subsection includes information subject to attorney-client
24 privilege or work product protection, the disclosure shall not
25 constitute a waiver of the privilege or protection.

26 (d) Comparison of processing operations.--A single data
27 protection assessment under subsection (a) may address a
28 comparable set of processing operations that include similar
29 activities.

30 (e) Compliance.--If a controller conducts a data protection

1 assessment for the purpose of complying with another applicable
2 Federal or State law or regulation, the data protection
3 assessment shall be deemed to satisfy the requirements under
4 this section if the data protection assessment is reasonably
5 similar in scope and effect to the data protection assessment
6 that would otherwise be conducted under this section.

7 (f) Applicability.--The data protection assessment
8 requirements under this section shall apply to processing
9 activities created or generated after July 1, 2024, and shall
10 not apply retroactively.

11 Section 8. De-identified and pseudonymous data.

12 (a) Duties.--A controller in possession of de-identified
13 data shall have the following duties:

14 (1) Take reasonable measures to ensure that the de-
15 identified data cannot be associated with an individual.

16 (2) Publicly commit to maintaining and using de-
17 identified data without attempting to re-identify the data.

18 (3) Contractually obligate a recipient of the de-
19 identified data to comply with the provisions of this act.

20 (b) Construction.--Nothing in this act shall be construed to
21 require a controller or processor to:

22 (1) require a controller or processor to re-identify de-
23 identified data or pseudonymous data;

24 (2) maintain data in identifiable form or collect,
25 obtain, retain or access data or technology in order to be
26 capable of associating an authenticated consumer rights
27 request under section 3(a); or

28 (3) comply with an authenticated consumer rights request
29 under section 3(a) if the controller:

30 (i) is not reasonably capable of associating the

1 request with the personal data, or it would be
2 unreasonably burdensome for the controller to associate
3 the request with the consumer's personal data;

4 (ii) does not use the personal data to recognize or
5 respond to the specific consumer who is the subject of
6 the personal data or does not associate the personal data
7 with other personal data about the same specific
8 consumer; and

9 (iii) does not sell the personal data to a third
10 party or otherwise voluntarily disclose the personal data
11 to a third party other than a processor, except as
12 authorized under this section.

13 (c) Pseudonymous data.--The consumer rights specified under
14 section 3(a)(1), (2), (3) or (4) shall not apply to pseudonymous
15 data if a controller is able to demonstrate that any information
16 necessary to identify the consumer is kept separately and is
17 subject to effective technical and organizational controls that
18 prevent the controller from accessing the information.

19 (d) Oversight.--A controller that discloses pseudonymous
20 data or de-identified data shall exercise reasonable oversight
21 to monitor compliance with a contractual commitment to which the
22 pseudonymous data or de-identified data is subject and shall
23 take appropriate steps to address a breach of the contractual
24 commitment.

25 Section 9. Exemptions on restrictions for controllers or
26 processors.

27 (a) Legal compliance.--Nothing in this act shall be
28 construed to restrict the ability of a controller or processor
29 to:

- 30 (1) comply with Federal or State laws or local

1 ordinances or regulations;

2 (2) comply with a civil, criminal or regulatory inquiry,
3 investigation, subpoena or summons by a Federal, State,
4 municipal or other governmental authority;

5 (3) cooperate with a law enforcement agency concerning a
6 conduct or activity that the controller or processor
7 reasonably and in good faith believes may violate a Federal
8 or State law or local ordinance or regulation;

9 (4) investigate, establish, exercise, prepare for or
10 defend legal claims;

11 (5) provide a product or service specifically requested
12 by a consumer;

13 (6) perform under a contract to which a consumer is a
14 party, including fulfilling the terms of a written warranty;

15 (7) take steps at the request of a consumer prior to
16 entering into a contract;

17 (8) take immediate steps to protect an interest that is
18 essential for the life or physical safety of a consumer or
19 another individual, including when processing cannot be
20 manifestly based on the provisions of this act;

21 (9) prevent, detect, protect against or respond to a
22 security incident, identity theft, fraud, harassment,
23 malicious or deceptive activity or illegal activity, preserve
24 the integrity or security of a system or investigate, report
25 or prosecute an individual responsible for an incident
26 specified under this paragraph;

27 (10) engage in public or peer-reviewed scientific or
28 statistical research in the public interest that adheres to
29 all other applicable Federal or State ethics and privacy laws
30 and is approved, monitored and governed by an institutional

1 review board or a similar independent oversight entity that
2 determines whether:

3 (i) the deletion of information is likely to provide
4 substantial benefits to the research that do not
5 exclusively accrue to the controller;

6 (ii) the expected benefits of the research outweigh
7 the privacy risks; and

8 (iii) the controller has implemented reasonable
9 safeguards to mitigate privacy risks associated with the
10 research, including risks associated with re-
11 identification;

12 (11) assist another controller, processor or third party
13 with any of the requirements under this act; or

14 (12) process personal data for reasons of public
15 interest in the area of public health, community health or
16 population health, but solely to the extent that the
17 processing is:

18 (i) subject to suitable and specific measures to
19 safeguard the rights of the consumer whose personal data
20 is being processed; and

21 (ii) under the responsibility of a professional
22 subject to confidentiality obligations under Federal or
23 State law or local ordinance.

24 (b) Data collection.--The requirements imposed on a
25 controller or processor under this act shall not restrict the
26 ability of a controller or processor to collect, use or retain
27 data for internal use for any of the following purposes:

28 (1) Conducting internal research to develop, improve or
29 repair products, services or technology.

30 (2) Effectuating a product recall.

1 (3) Identifying and repairing technical errors that
2 impair existing or intended functionality.

3 (4) Internal operations that are reasonably aligned with
4 the expectations of a consumer or reasonably anticipated
5 based on the consumer's existing relationship with the
6 controller or are otherwise compatible with processing data
7 in furtherance of the provision of a product or service
8 specifically requested by a consumer.

9 (c) Evidentiary privilege.--The requirements imposed on a
10 controller or processor under this act shall not apply if
11 compliance by the controller or processor with requirements
12 would violate an evidentiary privilege under the laws of this
13 Commonwealth. Nothing in this act shall be construed to prevent
14 a controller or processor from providing personal data
15 concerning a consumer to an individual covered by an evidentiary
16 privilege under the laws of this Commonwealth as part of a
17 privileged communication.

18 (d) Third parties.--A controller or processor that discloses
19 personal data to a third-party controller or third-party
20 processor in accordance with this act shall not be deemed to
21 have violated the provisions of this act if the third-party
22 controller or third-party processor violates the provisions of
23 this act if, at the time of the disclosure, the disclosing
24 controller or processor did not have actual knowledge that the
25 third-party controller or third-party processor would violate
26 the provisions of this act. A third-party controller or third-
27 party processor who receives personal data under this subsection
28 in accordance with this act shall not be deemed to have violated
29 the provisions of this act for a violation by the disclosing
30 controller or processor.

1 (e) Individual liberties.--Nothing in this act shall be
2 construed to:

3 (1) impose an obligation on a controller or processor
4 that adversely affects the rights or freedoms of an
5 individual, including the freedom of speech or freedom of the
6 press guaranteed in the First Amendment to the Constitution
7 of the United States or section 7 of Article I of the
8 Constitution of Pennsylvania; or

9 (2) apply to an individual's processing of personal data
10 in the course of the individual's purely personal or
11 household activities.

12 (f) Personal data.--

13 (1) Personal data processed by a controller may be
14 processed to the extent that the processing meets all of the
15 following criteria:

16 (i) Is reasonably necessary and proportionate to the
17 purposes specified under this section.

18 (ii) Is adequate, relevant and limited to what is
19 necessary in relation to the specific purposes specified
20 under this section.

21 (2) A controller or processor that collects, uses or
22 retains personal data under subsection (b) shall, when
23 applicable, take into account the nature and purpose of the
24 collection, use or retention of the personal data. The
25 personal data under subsection (b) shall be subject to
26 reasonable administrative, technical and physical measures to
27 protect the confidentiality, integrity and accessibility of
28 the personal data and reduce reasonably foreseeable risks of
29 harm to a consumer related to the collection, use or
30 retention of the personal data.

1 (g) Exemptions.--If a controller processes personal data in
2 accordance with an exemption under this section, the controller
3 shall be responsible for demonstrating that the processing
4 qualifies for the exemption and complies with the requirements
5 under subsection (f).

6 (h) Legal entities.--The processing of personal data for the
7 purposes expressly specified under this section shall not solely
8 make a legal entity a controller with respect to the processing.
9 Section 10. Penalties, enforcement and private rights of
10 action.

11 (a) Enforcement.--The Attorney General shall have exclusive
12 authority to enforce the provisions of this act. The following
13 shall apply:

14 (1) During the period beginning July 1, 2024, and ending
15 December 31, 2025, the Attorney General shall, prior to
16 initiating an action for a violation of a provision of this
17 act, issue a notice of violation to the controller or
18 processor if the Attorney General determines that a cure is
19 possible. If the controller fails to cure the violation
20 within 60 days of receipt of the notice of violation, the
21 Attorney General may initiate an action under this section.

22 (2) Beginning January 1, 2026, the Attorney General may,
23 in determining whether to grant a controller or processor the
24 opportunity to cure an alleged violation under paragraph (1),
25 consider all of the following:

26 (i) The number of violations.

27 (ii) The size and complexity of the controller or
28 processor.

29 (iii) The nature and extent of the processing
30 activities of the controller or processor.

1 (iv) The substantial likelihood of injury to the
2 public.

3 (v) The safety of persons or property.

4 (vi) Whether the alleged violation was likely caused
5 by human or technical error.

6 (3) THE RIGHT TO CURE SHALL APPLY FOR 60 DAYS. <--

7 (b) Private rights of action.--Nothing in this act shall be
8 construed as providing the basis for a private right of action
9 for a violation of the provisions of this act.

10 (c) Unfair trade practice.--Violations of the provisions of
11 this act shall constitute "unfair methods of competition" and
12 "unfair or deceptive acts or practices" under the act of
13 December 17, 1968 (P.L.1224, No.387), known as the Unfair Trade
14 Practices and Consumer Protection Law, and shall be enforced
15 exclusively by the Attorney General.

16 ~~(d) Guidance.--A controller or third party may seek the~~ <--
17 ~~opinion of the Attorney General for guidance on how to comply~~
18 ~~with the provisions of this act.~~

19 ~~(e)~~ (D) Regulations.--The Attorney General shall promulgate <--
20 regulations necessary to implement this section.

21 Section 11. Nonapplicability, exemption and consent.

22 (a) Nonapplicability.--This act shall not apply to any of
23 the following:

24 (1) The Commonwealth or any of its political
25 subdivisions.

26 (2) A nonprofit organization.

27 (3) An institution of higher education.

28 (4) A national securities association that is registered
29 under 15 U.S.C. § 78o-3 (relating to registered securities
30 associations).

1 of 42 U.S.C. Ch. 117 (relating to encouraging good faith
2 professional review activities).

3 (7) Patient safety work product for the purposes of 42
4 U.S.C. Ch. 6A Subch. VII Pt. C (relating to patient safety
5 improvement).

6 (8) Information derived from any of the health care
7 related information exempt under this subsection that is de-
8 identified in accordance with the requirements for de-
9 identification under HIPAA.

10 (9) Information originating from and intermingled to be
11 indistinguishable with, or information treated in the same
12 manner as, information exempt under this subsection that is
13 maintained by a covered entity or business associate, program
14 or qualified service organization as specified in 42 U.S.C. §
15 290dd-2 (relating to confidentiality of records).

16 (10) Information used for public health activities and
17 purposes as authorized by HIPAA, community health activities
18 and population health activities.

19 (11) The collection, maintenance, disclosure, sale,
20 communication or use of personal information bearing on a
21 consumer's credit worthiness, credit standing, credit
22 capacity, character, general reputation, personal
23 characteristics or mode of living by a consumer reporting
24 agency, furnisher or user that provides information for use
25 in a consumer report or by a user of a consumer report, but
26 only to the extent that the activity is regulated by and
27 authorized under 15 U.S.C. Ch. 41 Subch. III (relating to
28 credit reporting agencies).

29 (12) Personal data collected, processed, sold or
30 disclosed in compliance with 18 U.S.C. Ch. 123 (relating to

1 prohibition on release and use of certain personal
2 information from state motor vehicle records).

3 (13) Personal data regulated by 20 U.S.C. Ch. 31 Subch.
4 III Pt. 4 (relating to records; privacy; limitation on
5 withholding Federal funds).

6 (14) Personal data collected, processed, sold or
7 disclosed in compliance with 12 U.S.C. Ch. 23 (relating to
8 farm credit system).

9 (15) Data processed or maintained:

10 (i) in the course of an individual applying to,
11 employed by or acting as an agent or independent
12 contractor of a controller, processor or third party to
13 the extent that the data is collected and used within the
14 context of that role;

15 (ii) as the emergency contact information of an
16 individual specified under this act and used for
17 emergency contact purposes; or

18 (iii) as necessary to administer benefits for
19 another individual related to an individual who is the
20 subject of the information under paragraph (1) and used
21 for the purposes of administering the benefits.

22 (16) Personal data collected, processed, sold or
23 disclosed in relation to price, route or service by an air
24 carrier under 49 U.S.C. Subt. VII Pt. A. Subpt. I Ch. 401
25 (relating to general provisions) to the extent preempted
26 under 49 U.S.C. § 41713 (relating to preemption of authority
27 over prices, routes, and service).

28 (c) Parental consent.--A controller or processor that
29 complies with the verifiable parental consent requirements under
30 15 U.S.C. Ch. 91 (relating to children's online privacy

1 protection) shall be deemed compliant with an obligation to
2 obtain parental consent under this act.

3 Section 12. Effective date.

4 This act shall take effect ~~immediately~~ IN SIX MONTHS.

<--