

THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE BILL

No. 78 Session of 2025

INTRODUCED BY NEILSON, SCIALABBA, HOWARD, MENTZER, LEADBETER, SANCHEZ, HILL-EVANS, GIRAL, FRANKEL, KHAN, ARMANINI, WARREN, FREEMAN, OTTEN, ZIMMERMAN, GILLEN AND CIRESI, JANUARY 14, 2025

AS REPORTED FROM COMMITTEE ON COMMERCE, HOUSE OF REPRESENTATIVES, AS AMENDED, MARCH 18, 2025

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

1 fingerprints, voiceprints, eye retinas, irises or other unique
2 biological patterns or characteristics that are used to identify
3 a specific individual. The term does not include a digital or
4 physical photograph, an audio or video recording or any data
5 generated from a digital or physical photograph or an audio or
6 video recording. The term does not include information captured
7 and converted to a mathematical representation, including a
8 numeric string or similar method that cannot be used to recreate
9 the data captured or converted to create the mathematical
10 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) Alone or jointly with others, determines the
22 purposes and means of the processing of consumers'
23 personal information.

24 (iii) Does business in this Commonwealth.

25 (iv) Satisfies any of the following thresholds:

26 (A) Has annual gross revenues in excess of
27 \$10,000,000.

28 (B) Alone or in combination, annually buys or
29 receives, sells or shares for commercial purposes,
30 alone or in combination, the personal information of

1 at least 50,000 consumers, households or devices.

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

4 (2) An entity that controls a sole proprietorship,
5 partnership, limited liability company, corporation,
6 association or other legal entity under paragraph (1) or
7 shares common branding with the sole proprietorship,
8 partnership, limited liability company, corporation,
9 association or other legal entity.

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

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

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

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

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

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

1 (3) Contractually obligates a recipient of the data to
2 satisfy the criteria specified under paragraphs (1) and (2).
3 "HIPAA." The Health Insurance Portability and Accountability
4 Act of 1996 (Public Law 104-191, 110 Stat. 1936).

5 "Identified or identifiable individual." An individual who
6 can be readily identified, directly or indirectly.

7 "Institution of higher education." As defined in section
8 118(c) of the act of March 10, 1949 (P.L.30, No.14), known as
9 the Public School Code of 1949.

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

14 "Personal data." As follows:

15 (1) Any information that is linked or reasonably
16 linkable to an identified or identifiable individual.

17 (2) The term does not include publicly available
18 information, de-identified data or biometric data captured
19 and converted to a mathematical representation.

20 "Precise geolocation data." Information derived from
21 technology, including global positioning system level latitude
22 and longitude coordinates or other mechanisms, that directly
23 identifies the specific location of an individual with precision
24 and accuracy within a radius of 1,750 feet. The term does not
25 include the content of communications, or any data generated by
26 or connected to advanced utility metering infrastructure systems
27 or equipment for use by a utility.

28 "Process" or "processing." An operation or set of operations
29 performed, whether by manual or automated means, on personal
30 data or on sets of personal data, including the collection, use,

1 storage, disclosure, analysis, deletion or modification of
2 personal data.

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

5 (1) The processing of personal data for the purpose of
6 targeted advertising.

7 (2) The sale of personal data.

8 (3) The processing of personal data for the purpose of
9 profiling if the profiling presents a reasonably foreseeable
10 risk of any of the following:

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

13 (ii) Financial, physical or reputational injury to a
14 consumer.

15 (iii) A physical or other intrusion upon the
16 solitude or seclusion of a consumer or the private
17 affairs or concerns of a consumer where the intrusion
18 would be offensive to a reasonable person.

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

20 (4) The processing of sensitive data.

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

23 "Profiling." Any form of automated processing performed on
24 personal data to evaluate, analyze or predict personal aspects
25 related to an identified or identifiable individual's economic
26 situation, health, personal preferences, interests, reliability,
27 behavior, location or movements.

28 "Protected health information." As defined in 45 CFR
29 160.103.

30 "Pseudonymous data." Personal data that cannot be attributed

1 to a specific individual without the use of additional
2 information if the additional information is kept separately and
3 is subject to appropriate technical and organizational measures
4 to ensure that the personal data is not attributed to an
5 identified or identifiable individual.

6 "Publicly available information."

7 Information that:

8 (1) is lawfully available through Federal, State or
9 municipal records or widely distributed media; or

10 (2) a controller has a reasonable basis to believe a
11 consumer has lawfully made available to the general public.

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

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

17 (2) The disclosure of personal data to a third party for
18 the purpose of providing a product or service requested by a
19 consumer.

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

22 (4) The disclosure of personal data when a consumer
23 directs the controller to disclose the personal data or
24 intentionally uses the controller to interact with a third
25 party.

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

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

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

30 (6) The disclosure or transfer of personal data to a

1 third party as an asset that is part of a merger,
2 acquisition, bankruptcy or other transaction or a proposed
3 merger, acquisition, bankruptcy or other transaction, in
4 which the third party assumes control of all or part of the
5 controller's assets.

6 "Sensitive data." Personal data that includes data revealing
7 any of the following:

8 (1) A racial or ethnic origin.

9 (2) Religious beliefs.

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

11 (4) Sex life or sexual orientation.

12 (5) Citizenship or immigration status.

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

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

16 (8) Precise geolocation data.

17 "Targeted advertising." Displaying advertisements to a
18 consumer if the advertisement is selected based on personal data
19 obtained or inferred from the consumer's activities over time
20 and across nonaffiliated Internet websites or online
21 applications to predict the consumer's preferences or interests.

22 The term does not include any of the following:

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

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

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

30 (4) Processing personal data solely to measure or report

1 advertising frequency, performance or reach.

2 "Third party." An individual or legal entity, including a
3 public authority, agency or body, other than a consumer,
4 controller or processor or an affiliate of the processor or the
5 controller.

6 "Trade secret." As defined in 12 Pa.C.S. § 5302 (relating to
7 definitions).

8 Section 3. Consumer data privacy.

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

11 (1) Confirm whether or not a controller is processing or
12 accessing the consumer's personal data, unless the
13 confirmation or access would require the controller to reveal
14 a trade secret.

15 (2) Correct inaccuracies in the consumer's personal
16 data, taking into account the nature of the personal data and
17 the purposes of the processing of the consumer's personal
18 data.

19 (3) Delete personal data provided by or obtained about
20 the consumer.

21 (4) Obtain a copy of the consumer's personal data
22 processed by a controller in a portable and, to the extent
23 technically feasible, readily usable format that allows the
24 consumer to transmit the data to another controller without
25 hindrance, where the processing is carried out by automated
26 means in a manner that would disclose the controller's trade
27 secrets.

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

30 (i) Targeted advertising.

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

3 (iii) Profiling in furtherance of solely automated
4 decisions that produce legal or similarly significant
5 effects concerning the consumer.

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

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

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

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

6 (3) Information provided in response to consumer
7 requests shall be provided by the controller, free of charge,
8 once per consumer during a 12-month period. If a request from
9 a consumer is manifestly unfounded, excessive or repetitive,
10 the controller may charge the consumer a reasonable fee to
11 cover the administrative costs of complying with the request
12 or decline to act on the request. The controller bears the
13 burden of demonstrating the manifestly unfounded, excessive
14 or repetitive nature of the request.

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

1 person who made the request disclosing that the controller
2 believes the request is fraudulent, why the controller
3 believes the request is fraudulent and that the controller
4 will not comply with the request.

5 (5) A controller that has obtained personal data about a
6 consumer from a source other than the consumer shall be
7 deemed in compliance with a consumer's request to delete the
8 personal data in accordance with subsection (a)(3) by
9 retaining a record of the deletion request and the minimum
10 data necessary for the purpose of ensuring that the
11 consumer's personal data remains deleted from the
12 controller's records and not using such retained data for any
13 other purpose in accordance with the provisions of this act
14 or opting the consumer out of the processing of the data for
15 any purpose except for those exempted under section 11(a)(3).

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

1 Section 4. Designation of authorized agent.

2 A consumer may designate another person to serve as the
3 consumer's authorized agent and act on the consumer's behalf to
4 opt out of the processing of the consumer's personal data for
5 the purposes specified under section 3(a)(5). A controller shall
6 comply with an opt-out request received from an authorized agent
7 under section 3(a)(5) if the controller is able to verify, with
8 commercially reasonable effort, the identity of the consumer and
9 the authorized agent's authority to act on the consumer's
10 behalf.

11 Section 5. Duties of controllers.

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

14 (1) Limit the collection of personal data to what is
15 adequate, relevant and reasonably necessary in relation to
16 the purposes for which the data is processed, as disclosed to
17 the consumer.

18 (2) Except as otherwise provided in this act, refrain
19 from processing personal data for purposes that are neither
20 reasonably necessary to, nor compatible with, the disclosed
21 purposes for which the personal data is processed, as
22 disclosed to the consumer, unless the controller obtains the
23 consumer's consent.

24 (3) Process personal data in a manner that ensures
25 reasonable and appropriate administrative, technical,
26 organizational and physical safeguards of personal data
27 collected, stored and processed.

28 (4) Refrain from processing sensitive data concerning a
29 consumer without obtaining the consumer's consent or, in the
30 case of the processing of sensitive data concerning a known

1 child, without processing the data, in accordance with 15
2 U.S.C. Ch. 91 (relating to children's online privacy
3 protection).

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

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

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

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

25 (b) Construction.--Nothing in subsection (a) shall be
26 construed to require a controller to provide a product or
27 service that requires the personal data of a consumer that the
28 controller does not collect or maintain nor prohibit a
29 controller from offering a different price, rate, level, quality
30 or selection of goods or services to a consumer, including

1 offering goods or services for no fee, if the offering is in
2 connection with a consumer's voluntary participation in a bona
3 fide loyalty, rewards, premium features, discounts or club card
4 program.

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

8 (1) The categories of personal data processed by the
9 controller.

10 (2) The purpose for processing personal data.

11 (3) How the consumer may exercise the consumer's rights,
12 including how the consumer may appeal the controller's
13 decision with regard to the consumer's request under section
14 3(d).

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

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

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

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

26 (e) Means to exercise rights.--

27 (1) A controller shall establish and describe in the
28 privacy notice under subsection (c) a secure and reliable
29 means for consumers to submit a request to exercise the
30 consumer's rights under section 3(a). The secure and reliable

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

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

15 (ii) No later than ~~January 1, 2027~~ JANUARY 1 OF THE <--
16 YEAR COMMENCING TWO YEARS AFTER THE EFFECTIVE DATE OF
17 THIS SUBPARAGRAPH, allowing a consumer to opt out of the
18 processing of the consumer's personal data for the
19 purpose of targeted advertising or the sale of the
20 consumer's personal data under section 3(a)(5) through an
21 opt-out preference signal sent, with the consumer's
22 consent, by a platform, technology or mechanism to the
23 controller indicating the consumer's intent to opt out of
24 the processing or sale. The platform, technology or
25 mechanism shall comply with all of the following
26 criteria:

27 (A) Not unfairly disadvantage another
28 controller.

29 (B) Not make use of a default setting, but
30 instead require the consumer to make an affirmative,

1 freely given and unambiguous choice to opt out of the
2 processing or sale of the consumer's personal data.

3 (C) Be consumer friendly and easy to use by the
4 average consumer.

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

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

13 (F) Be in compliance with this section. A
14 controller that recognizes signals approved by other
15 states shall be considered in compliance with this
16 section.

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

1 (2) If a controller responds to a consumer's opt-out
2 request under paragraph (1)(i) by informing the consumer of a
3 charge for the use of a product or service, the controller
4 shall present the terms of a bona fide loyalty, rewards,
5 premium features, discounts or club card program for the
6 retention, use, sale or sharing of the consumer's personal
7 data.

8 Section 6. Duties of processors.

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

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

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

25 (3) Providing necessary information to enable the
26 controller to conduct and document data protection
27 assessments.

28 (b) Contracts.--A contract between a controller and a
29 processor shall govern the processor's data processing
30 procedures with respect to processing performed on behalf of the

1 controller. The contract shall be binding and clearly state the
2 instructions for processing data, the nature and purpose of
3 processing, the type of data subject to processing, the duration
4 of processing and the rights and obligations of both parties.
5 The contract shall also require that the processor comply with
6 all of the following:

7 (1) Ensure that each person processing personal data is
8 subject to a duty of confidentiality with respect to the
9 data.

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

14 (3) Upon the reasonable request of the controller, make
15 available to the controller all information in the
16 processor's possession necessary to demonstrate the
17 processor's compliance with the provisions of this act.

18 (4) After providing the controller with an opportunity
19 to object, engage a subcontractor pursuant to a written
20 contract that requires the subcontractor to meet the
21 obligations of the processor with respect to the personal
22 data.

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

1 controller upon request.

2 (c) Construction.--Nothing in this section shall be
3 construed to relieve a controller or processor from the
4 liabilities imposed on the controller or processor by virtue of
5 the role of the controller or processor in the processing
6 relationship specified under this act.

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

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

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

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

25 Section 7. Data protection assessment.

26 (a) Assessment.--A controller shall conduct and document a
27 data protection assessment for each of the controller's
28 processing activities that present a heightened risk of harm to
29 a consumer.

30 (b) Benefits and risks.--In conducting a data protection

1 assessment under subsection (a), a controller shall identify and
2 weigh the benefits that may flow, directly and indirectly, from
3 the processing to the controller, the consumer, other
4 stakeholders and the public against the potential risks to the
5 consumer's rights under section 3(a) associated with the
6 processing, as mitigated by safeguards that can be employed by
7 the controller to reduce the risks. The controller shall factor
8 all of the following into the data protection assessment:

9 (1) The use of de-identified data.

10 (2) The reasonable expectations of the consumer.

11 (3) The context of the processing and the relationship
12 between the controller and the consumer whose personal data
13 will be processed.

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

30 (d) Comparison of processing operations.--A single data

1 protection assessment under subsection (a) may address a
2 comparable set of processing operations that includes similar
3 activities.

4 (e) Compliance.--If a controller conducts a data protection
5 assessment for the purpose of complying with another applicable
6 Federal or State law or regulation, the data protection
7 assessment shall be deemed to satisfy the requirements under
8 this section if the data protection assessment is reasonably
9 similar in scope and effect to the data protection assessment
10 that would otherwise be conducted under this section.

11 (f) Applicability.--The data protection assessment
12 requirements under this section shall apply to processing
13 activities created or generated after ~~July 1, 2025,~~ JULY 1 OF <--
14 THE YEAR COMMENCING ONE YEAR AFTER THE EFFECTIVE DATE OF THIS
15 SUBSECTION and shall not apply retroactively.

16 Section 8. De-identified data and pseudonymous data.

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

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

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

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

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

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

29 (2) maintain data in identifiable form or collect,
30 obtain, retain or access data or technology in order to be

1 capable of associating an authenticated consumer rights
2 request under section 3(a); or

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

5 (i) is not reasonably capable of associating the
6 request with the personal data, or it would be
7 unreasonably burdensome for the controller to associate
8 the request with the consumer's personal data;

9 (ii) does not use the personal data to recognize or
10 respond to the specific consumer who is the subject of
11 the personal data or does not associate the personal data
12 with other personal data about the same specific
13 consumer; and

14 (iii) does not sell the personal data to a third
15 party or otherwise voluntarily disclose the personal data
16 to a third party other than a processor, except as
17 authorized under this section.

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

24 (d) Oversight.--A controller that discloses pseudonymous
25 data or de-identified data shall exercise reasonable oversight
26 to monitor compliance with a contractual commitment to which the
27 pseudonymous data or de-identified data is subject and shall
28 take appropriate steps to address a breach of the contractual
29 commitment.

30 Section 9. Exemptions on restrictions for controllers or

1 processors.

2 (a) Legal compliance.--Nothing in this act shall be
3 construed to restrict the ability of a controller or processor
4 to:

5 (1) comply with Federal or State laws or local
6 ordinances or regulations;

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

10 (3) cooperate with a law enforcement agency concerning a
11 conduct or activity that the controller or processor
12 reasonably and in good faith believes may violate a Federal
13 or State law or local ordinance or regulation;

14 (4) investigate, establish, exercise, prepare for or
15 defend legal claims;

16 (5) provide a product or service specifically requested
17 by a consumer;

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

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

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

26 (9) prevent, detect, protect against or respond to a
27 security incident, identity theft, fraud, harassment,
28 malicious or deceptive activity or illegal activity, preserve
29 the integrity or security of a system or investigate, report
30 or prosecute an individual responsible for an incident

1 specified under this paragraph;

2 (10) engage in public or peer-reviewed scientific or
3 statistical research in the public interest that adheres to
4 all other applicable Federal or State ethics and privacy laws
5 and is approved, monitored and governed by an institutional
6 review board or a similar independent oversight entity that
7 determines whether:

8 (i) the deletion of information is likely to provide
9 substantial benefits to the research that do not
10 exclusively accrue to the controller;

11 (ii) the expected benefits of the research outweigh
12 the privacy risks; and

13 (iii) the controller has implemented reasonable
14 safeguards to mitigate privacy risks associated with the
15 research, including risks associated with re-
16 identification;

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

19 (12) process personal data for reasons of public
20 interest in the area of public health, community health or
21 population health, but solely to the extent that the
22 processing is:

23 (i) subject to suitable and specific measures to
24 safeguard the rights of the consumer whose personal data
25 is being processed; and

26 (ii) under the responsibility of a professional
27 subject to confidentiality obligations under Federal or
28 State law or local ordinance.

29 (b) Data collection.--The requirements imposed on a
30 controller or processor under this act shall not restrict the

1 ability of a controller or processor to collect, use or retain
2 data for internal use for any of the following purposes:

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

5 (2) Effectuating a product recall.

6 (3) Identifying and repairing technical errors that
7 impair existing or intended functionality.

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

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

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

1 the provisions of this act. A third-party controller or third-
2 party processor who receives personal data under this subsection
3 in accordance with this act shall not be deemed to have violated
4 the provisions of this act for a violation by the disclosing
5 controller or processor.

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

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

14 (2) apply to an individual's processing of personal data
15 in the course of the individual's purely personal or
16 household activities.

17 (f) Personal data.--

18 (1) Personal data processed by a controller may be
19 processed to the extent that the processing meets all of the
20 following criteria:

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

23 (ii) Is adequate, relevant and limited to what is
24 necessary in relation to the specific purposes specified
25 under this section.

26 (2) A controller or processor that collects, uses or
27 retains personal data under subsection (b) shall, when
28 applicable, take into account the nature and purpose of the
29 collection, use or retention of the personal data. The
30 personal data under subsection (b) shall be subject to

1 reasonable administrative, technical and physical measures to
2 protect the confidentiality, integrity and accessibility of
3 the personal data and reduce reasonably foreseeable risks of
4 harm to a consumer related to the collection, use or
5 retention of the personal data.

6 (g) Exemptions.--If a controller processes personal data in
7 accordance with an exemption under this section, the controller
8 shall be responsible for demonstrating that the processing
9 qualifies for the exemption and complies with the requirements
10 under subsection (f).

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

16 (a) Enforcement.--The Attorney General shall have exclusive
17 authority to enforce the provisions of this act. The following
18 shall apply:

19 (1) During the period beginning January 1, ~~2026~~, and <--
20 ending ~~July 1, 2026~~ JULY 1 OF THE YEAR COMMENCING ONE YEAR <--
21 AFTER THE EFFECTIVE DATE OF THIS PARAGRAPH, the Attorney
22 General shall, prior to initiating an action for a violation
23 of a provision of this act, issue a notice of violation to
24 the controller or processor if the Attorney General
25 determines that a cure is possible. If the controller fails
26 to cure the violation within 60 days of receipt of the notice
27 of violation, the Attorney General may initiate an action
28 under this section.

29 (2) Beginning ~~January 1, 2026~~ JANUARY 1 OF THE YEAR <--
30 COMMENCING ONE YEAR AFTER THE EFFECTIVE DATE OF THIS

1 PARAGRAPH, the Attorney General may, in determining whether
2 to grant a controller or processor the opportunity to cure an
3 alleged violation under paragraph (1), consider all of the
4 following:

5 (i) The number of violations.

6 (ii) The size and complexity of the controller or
7 processor.

8 (iii) The nature and extent of the processing
9 activities of the controller or processor.

10 (iv) The substantial likelihood of injury to the
11 public.

12 (v) The safety of persons or property.

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

15 (3) The right to cure shall apply for 60 days.

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

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

25 (d) Regulations.--The Attorney General shall promulgate
26 regulations necessary to implement this section.

27 Section 11. Nonapplicability, exemption and consent.

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

30 (1) The Commonwealth or any of its political

1 subdivisions.

2 (2) A nonprofit organization.

3 (3) An institution of higher education.

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

7 (5) A financial institution or an affiliate of a
8 financial institution or data subject to Title V of the
9 Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.).

10 (6) A covered entity or business associate.

11 (b) Exemptions.--The following shall be exempt from the
12 provisions of this act:

13 (1) Protected health information under HIPAA.

14 (2) Patient-identifying information for purposes of 42
15 U.S.C. § 290dd-2 (relating to confidentiality of records).

16 (3) Identifiable private information for purposes of the
17 Federal policy for the protection of human subjects under 45
18 CFR Subt. A Subch. A Pt. 46 (relating to protection of human
19 subjects).

20 (4) Identifiable private information that is otherwise
21 information collected as part of human subjects research in
22 accordance with the good clinical practice guidelines issued
23 by the International Council for Harmonisation of Technical
24 Requirements for Pharmaceuticals for Human Use on the
25 effective date of this paragraph.

26 (5) The protection of human subjects under 21 CFR Ch. I
27 Subch. A Pt. 50 (relating to protection of human subjects) or
28 56 (relating to institutional review boards) or personal data
29 used or shared in research, as defined in 45 CFR 164.501
30 (relating to definitions), that is conducted in accordance

1 with the standards specified under this subsection or other
2 research conducted in accordance with applicable Federal or
3 State law.

4 (6) Information and documents created for the purposes
5 of 42 U.S.C. Ch. 117 (relating to encouraging good faith
6 professional review activities).

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

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

14 (9) Information originating from and intermingled to be
15 indistinguishable with, or information treated in the same
16 manner as, information exempt under this subsection that is
17 maintained by a covered entity or business associate, program
18 or qualified service organization as specified in 42 U.S.C. §
19 290dd-2.

20 (10) Information used for public health activities and
21 purposes as authorized by HIPAA, community health activities
22 and population health activities.

23 (11) The collection, maintenance, disclosure, sale,
24 communication or use of personal information bearing on a
25 consumer's credit worthiness, credit standing, credit
26 capacity, character, general reputation, personal
27 characteristics or mode of living by a consumer reporting
28 agency, furnisher or user that provides information for use
29 in a consumer report or by a user of a consumer report, but
30 only to the extent that the activity is regulated by and

1 authorized under 15 U.S.C. Ch. 41 Subch. III (relating to
2 credit reporting agencies).

3 (12) Personal data collected, processed, sold or
4 disclosed in compliance with 18 U.S.C. Ch. 123 (relating to
5 prohibition on release and use of certain personal
6 information from state motor vehicle records).

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

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

13 (15) Data processed or maintained:

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

19 (ii) as the emergency contact information of an
20 individual specified under this act and used for
21 emergency contact purposes; or

22 (iii) as necessary to administer benefits for
23 another individual related to an individual who is the
24 subject of the information under paragraph (1) and used
25 for the purposes of administering the benefits.

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

1 over prices, routes, and service).

2 (c) Parental consent.--A controller or processor that
3 complies with the verifiable parental consent requirements under
4 15 U.S.C. Ch. 91 (relating to children's online privacy
5 protection) shall be deemed compliant with an obligation to
6 obtain parental consent under this act.

7 Section 12. Effective date.

8 This act shall take effect in ~~six months~~ ONE YEAR.

<--