

**SUBSTITUTE FOR
SENATE BILL NO. 659**

A bill to establish the privacy rights of consumers; to require certain persons to provide certain notices to consumers regarding the collection, processing, sale, sharing, and retention of personal data; to provide for a universal opt-out mechanism; to prohibit certain acts and practices concerning the collection, processing, sale, sharing, and retention of personal data; to establish standards and practices regarding the collection, processing, sale, sharing, and retention of personal data; to require the registration of data brokers; to provide for the powers and duties of certain state governmental officers and entities; to create certain funds; and to provide remedies.

THE PEOPLE OF THE STATE OF MICHIGAN ENACT:

1 Sec. 1. This act may be cited as the "personal data privacy



1 act".

2 Sec. 3. For purposes of this act, the words and phrases
3 defined in sections 5 to 9 have the meanings ascribed to them in
4 those sections. These definitions, unless the context otherwise
5 requires, apply to use of the defined terms in this act. Other
6 definitions applicable to specific sections of the act are found in
7 those sections.

8 Sec. 5. (1) "Affiliate" means a person that controls, is
9 controlled by, or is under common control with another person or
10 shares common branding with another person. As used in this
11 subsection, "control" or "controlled" means any of the following:

12 (a) Ownership of, or the power to vote, more than 50% of the
13 outstanding shares of any class of voting security of a company.

14 (b) Control in any manner over the election of a majority of
15 the directors or of individuals exercising similar functions.

16 (c) The power to exercise controlling influence over the
17 management of a company.

18 (2) "Authenticate" means verifying through reasonable means
19 that a consumer, entitled to exercise the consumer rights under
20 section 13, is the same consumer exercising those consumer rights
21 with respect to the personal data at issue.

22 (3) "Biometric data" means data generated by automatic
23 measurements of an individual's biological characteristics,
24 including, but not limited to, a fingerprint, a voiceprint, eye
25 retinas, irises, or other unique biological patterns or
26 characteristics, that can be used to identify a specific
27 individual. Biometric data does not include any of the following:

28 (a) A physical or digital photograph.

29 (b) A video or audio recording.



1 (c) Any data generated from a physical or digital photograph,
2 or a video or audio recording, unless the data is generated to
3 identify a specific individual.

4 (4) "Business associate" means that term as defined in 45 CFR
5 160.103

6 (5) "Child" means an individual who is less than 13 years of
7 age.

8 (6) "Collects", "collected", or "collection" means buying,
9 renting, gathering, obtaining, receiving, or accessing a consumer's
10 personal data by any means.

11 (7) "Consent" means a clear affirmative act signifying a
12 consumer's freely given, specific, informed, and unambiguous
13 agreement to process personal data relating to the consumer.
14 Consent may include a written statement, including a statement
15 written by electronic means, or any other unambiguous affirmative
16 action. Consent does not include any of the following:

17 (a) The acceptance of a general or broad terms of use or
18 similar document that contains any description of personal data
19 processing and other unrelated information.

20 (b) The act of hovering over, muting, pausing, or closing a
21 given piece of content.

22 (c) An agreement obtained through the use of dark patterns.

23 (8) "Consumer" means an individual who is a resident of this
24 state acting in an individual or household context. Consumer does
25 not include an individual acting in a commercial or employment
26 context.

27 (9) "Consumer health data" means personal data that a
28 controller uses to identify a consumer's physical or mental health
29 condition or diagnosis, including, but not limited to, gender-



1 affirming health data and reproductive or sexual health data.

2 (10) "Controller" means a person that, alone or jointly with
3 others, determines the purpose and means of processing personal
4 data.

5 (11) "Covered entity" means that term as defined in 45 CFR
6 160.103.

7 (12) "Dark pattern" means a user interface designed or
8 manipulated with the substantial effect of subverting or impairing
9 user autonomy, decision-making, or choice.

10 (13) "Data broker" means a company, or a unit or units of a
11 company, separately or together, that knowingly collects and sells,
12 or licenses to a third party, the brokered personal data of a
13 consumer with whom the company does not have a direct relationship.

14 (14) "Decisions that produce legal or similarly significant
15 effects concerning a consumer" means decisions that result in the
16 provision or denial of financial and lending services, housing,
17 insurance, education enrollment or opportunity, criminal justice,
18 employment opportunities, health care services, or access to basic
19 necessities, including, but not limited to, food and water.

20 (15) "De-identified data" means data that cannot reasonably be
21 linked to an identified or identifiable individual, or to a device
22 linked to that individual.

23 (16) "Financial institution" means either of the following:

24 (a) A state or nationally chartered bank or state or a
25 federally chartered savings and loan association, savings bank, or
26 credit union whose deposits are insured by an agency of the United
27 States government.

28 (b) An affiliate or subsidiary of an entity under subdivision
29 (a) that is primarily engaged in financial activities as described



1 in 12 USC 1843(k).

2 Sec. 7. (1) "Gender-affirming health data" means any personal
3 data concerning an effort made by a consumer to seek, or a
4 consumer's receipt of, gender-affirming health care services.

5 (2) "Geofence" means any technology that uses global
6 positioning coordinates, cell tower connectivity, cellular data,
7 radio frequency identification, wireless fidelity technology data,
8 or any other form of location detection, or any combination of the
9 coordinates, connectivity, data, identification, or other form of
10 location detection, to establish a virtual boundary.

11 (3) "Identified or identifiable individual" means an
12 individual who can be readily identified, directly or indirectly.

13 (4) "Institution of higher education" means a degree- or
14 certificate-granting public or private college or university,
15 junior college, or community college located in this state.

16 (5) "Institutional review board" means that term as defined in
17 21 CFR 56.102.

18 (6) "Mental health facility" means a health care facility in
19 which not less than 70% of the health care services provided in the
20 facility are mental health services.

21 (7) "Person" means an individual or a partnership,
22 corporation, limited liability company, association, governmental
23 entity, or other legal entity.

24 (8) "Personal data" means information that is linked or
25 reasonably linkable to an identified or identifiable individual.
26 Personal data does not include de-identified data or publicly
27 available information.

28 (9) "Precise geolocation data" means information derived from
29 technology, including, but not limited to, global positioning



1 system level latitude and longitude coordinates or other
2 mechanisms, that directly identifies the specific location of an
3 individual with precision and accuracy within a radius of 1,750
4 feet. Precise geolocation data does not include the content of
5 communications or data generated by or connected to advanced
6 utility metering infrastructure systems or equipment for use by a
7 utility.

8 (10) "Process" or "processing" means an operation or set of
9 operations performed, whether by manual or automated means, on
10 personal data or on sets of personal data, including, but not
11 limited to, the collection, use, storage, disclosure, analysis,
12 deletion, or modification of personal data.

13 (11) "Processor" means a person that processes personal data
14 on behalf of a controller.

15 (12) "Profiling" means any form of automated processing
16 performed on personal data to evaluate, analyze, or predict
17 personal aspects related to an identified or identifiable
18 individual's economic situation, health, personal preferences,
19 interests, reliability, behavior, location, or movements.

20 (13) "Pseudonymous data" means personal data that cannot be
21 attributed to a specific individual without the use of additional
22 information, if the additional information is kept separately and
23 is subject to appropriate technical and organizational measures to
24 ensure that the personal data is not attributed to an identified or
25 identifiable individual.

26 (14) "Publicly available information" means information that
27 is lawfully made available through federal, state, or local
28 government records, or information that a person has a reasonable
29 basis to believe is lawfully made available to the general public



1 through widely distributed media, by the consumer, or by a person
2 to whom the consumer has disclosed the information, unless the
3 consumer has restricted the information to a specific audience.

4 Sec. 9. (1) "Reproductive or sexual health care" means any
5 health-care-related services or products rendered or provided
6 concerning a consumer's reproductive system or sexual well-being,
7 including, but not limited to, any service or product rendered or
8 provided concerning any of the following:

9 (a) An individual health condition, status, disease,
10 diagnosis, diagnostic test, or treatment.

11 (b) A social, psychological, behavioral, or medical
12 intervention.

13 (c) A surgery or procedure, including, but not limited to, an
14 abortion.

15 (d) A use or purchase of a medication, including, but not
16 limited to, a medication used or purchased for the purposes of an
17 abortion.

18 (e) A bodily function, vital sign, or symptom.

19 (f) A measurement of a bodily function, vital sign, or
20 symptom.

21 (g) An abortion, including, but not limited to, medical or
22 nonmedical services, products, diagnostics, counseling, or follow-
23 up services for an abortion.

24 (2) "Reproductive or sexual health data" means personal data
25 concerning an effort made by a consumer to seek, or a consumer's
26 receipt of, reproductive or sexual health care.

27 (3) "Reproductive or sexual health facility" means a health
28 care facility in which not less than 70% of the health care
29 services or products provided are reproductive or sexual health



1 care.

2 (4) "Sale of personal data" means the exchange of personal
3 data for monetary or other valuable consideration by a controller
4 to a third party. Sale of personal data does not include any of the
5 following:

6 (a) The disclosure of personal data to a processor that
7 processes the personal data on behalf of the controller.

8 (b) The disclosure of personal data to a third party for the
9 purpose of providing a product or service requested by the
10 consumer.

11 (c) The disclosure or transfer of personal data to an
12 affiliate of the controller.

13 (d) The disclosure of information that the consumer
14 intentionally made available to the general public via a channel of
15 mass media and did not restrict the information to a specific
16 audience.

17 (e) The disclosure or transfer of personal data to a third
18 party as an asset that is part of a merger, acquisition,
19 bankruptcy, or other transaction, or a proposed merger,
20 acquisition, bankruptcy, or other transaction, in which the third
21 party assumes or will assume control of all or part of the
22 controller's assets.

23 (5) "Sensitive data" means a category of personal data that
24 includes all of the following:

25 (a) Personal data revealing racial or ethnic origin, religious
26 beliefs, mental or physical health diagnosis, sexual orientation,
27 or citizenship or immigration status.

28 (b) Genetic or biometric data for the purpose of uniquely
29 identifying an individual.



1 (c) Personal data collected from a known child.

2 (d) Precise geolocation data.

3 (e) Consumer health data.

4 (6) "State agency" means a state department, agency, bureau,
5 division, section, board, commission, trustee, authority, or
6 officer that is created by the state constitution of 1963, statute,
7 or state agency action.

8 (7) "Subprocessor" means a person that has a contract with a
9 processor to process personal data that is subject to a contract
10 between the processor and a controller.

11 (8) "Targeted advertising" means displaying advertisements to
12 a consumer if the advertisements are selected based on personal
13 data obtained or inferred from that consumer's activities over time
14 and across nonaffiliated websites or online applications to predict
15 the consumer's preferences or interests. Targeted advertising does
16 not include any of the following:

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

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

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

23 (d) Processing personal data solely for the purpose of
24 measuring or reporting advertising performance, reach, or
25 frequency.

26 (9) "Third party" means a person other than the consumer,
27 controller, processor, subprocessor, or an affiliate of the
28 controller or processor.

29 (10) "Trade secret" means that term as defined in section 2 of



1 the uniform trade secrets act, 1998 PA 448, MCL 445.1902.

2 Sec. 11. (1) This act applies to a person that does both of
3 the following:

4 (a) Conducts business in this state or produces products or
5 services that are targeted to residents of this state.

6 (b) During a calendar year, does either of the following:

7 (i) Controls or processes personal data of at least 100,000
8 consumers.

9 (ii) Controls or processes personal data of at least 25,000
10 consumers and derives any revenue from the sale of personal data.

11 (2) This act does not apply to any of the following:

12 (a) A state agency or any other political subdivision of this
13 state.

14 (b) A covered entity or business associate governed by the
15 privacy, security, and breach notification rules under the health
16 insurance portability and accountability act of 1996, Public Law
17 104-191, and the regulations promulgated under that act, 45 CFR
18 parts 160 and 164, and the health information technology for
19 economic and clinical health act, Public Law 111-5.

20 (c) An institution of higher education.

21 (d) A financial institution.

22 (e) An entity that is subject to or regulated under the
23 insurance code of 1956, 1956 PA 218, MCL 500.100 to 500.8302.

24 (f) A nonprofit organization that operates to detect or
25 prevent insurance-related crimes, including, but not limited to,
26 insurance fraud.

27 (g) A nonprofit dental care corporation operating under 1963
28 PA 125, MCL 550.351 to 550.373.

29 (h) A third party administrator as that term is defined in



1 section 2 of the third party administrator act, 1984 PA 218, MCL
2 550.902.

3 (3) The following information and data are exempt from this
4 act:

5 (a) Protected health information under the health insurance
6 portability and accountability act of 1996, Public Law 104-191, and
7 the regulations promulgated under that act, 45 CFR parts 160 and
8 164.

9 (b) Information that is maintained by a health care provider,
10 as that term is defined in 45 CFR 160.103, if the health care
11 provider maintains the information in the manner required by a
12 covered entity with respect to protected health information under
13 the health insurance portability and accountability act of 1996,
14 Public Law 104-191, and the regulations promulgated under that act.

15 (c) A record that is a medical record as that term is defined
16 in section 3 of the medical records access act, 2004 PA 47, MCL
17 333.26263.

18 (d) Patient identifying information for purposes of 42 USC
19 290dd-2.

20 (e) Identifiable private information for the purpose of the
21 federal policy for the protection of human subjects under 45 CFR
22 part 46; identifiable private information that is otherwise
23 information collected as part of human subjects research in
24 accordance with the "Good Clinical Practice Guidelines" issued by
25 the International Council for Harmonisation of Technical
26 Requirements for Pharmaceuticals for Human Use; the protection of
27 human subjects under 21 CFR parts 50 and 56; and personal data used
28 or shared in research conducted in accordance with the requirements
29 under this act, or other research conducted in accordance with



1 applicable law.

2 (f) Information and documents created for purposes of the
3 health care quality improvement act of 1986, 42 USC 11101 to 11152.

4 (g) Patient safety work product for purposes of the patient
5 safety and quality improvement act of 2005, Public Law 109-41.

6 (h) Information derived from any of the health care-related
7 information listed in this subsection that is de-identified in
8 accordance with the requirements for de-identification under the
9 health insurance portability and accountability act of 1996, Public
10 Law 104-191.

11 (i) Information originating from, and intermingled to be
12 indistinguishable with, or information treated in the same manner
13 as information exempt under this subsection that is maintained by a
14 covered entity, business associate, program, or qualified service
15 organization. As used in this subdivision, "program" and "qualified
16 service organization" mean those terms as defined in 42 CFR 2.11.

17 (j) Information used only for public health activities and
18 purposes as authorized under the health insurance portability and
19 accountability act of 1996, Public Law 104-191.

20 (k) The collection, maintenance, disclosure, sale,
21 communication, or use of any personal data bearing on a consumer's
22 creditworthiness, credit standing, credit capacity, character,
23 general reputation, personal characteristics, or mode of living by
24 a consumer reporting agency, furnisher, or user that provides
25 information for use in a consumer report, and by a user of a
26 consumer report, but only to the extent that the activity is
27 regulated by and authorized under the fair credit reporting act, 15
28 USC 1681 to 1681x.

29 (l) Personal data collected, processed, sold, or disclosed in



1 compliance with the driver's privacy protection act of 1994, 18 USC
2 2721 to 2725.

3 (m) Personal data regulated by the family educational rights
4 and privacy act of 1974, 20 USC 1232g.

5 (n) Personal data collected, processed, sold, or disclosed in
6 compliance with 12 USC 2001 to 2279cc.

7 (o) Data processed or maintained for any of the following
8 purposes:

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

13 (ii) As the emergency contact information of an individual for
14 emergency contact purposes.

15 (iii) That is necessary to retain to administer benefits for
16 another individual relating to the individual under subparagraph (i)
17 and used for the purpose of administering those benefits.

18 (iv) That is necessary in any matter relating to an
19 unemployment benefit claim or appeal under the Michigan employment
20 security act, 1936 (Ex Sess) PA 1, MCL 421.1 to 421.75.

21 (p) Data that is subject to title V of the Gramm-Leach-Bliley
22 act, 15 USC 6801 to 6827, and the regulations promulgated under
23 that act.

24 (q) Information or data that are collected or obtained for the
25 sole purpose of developing, testing, or operating an automated
26 driving system or advanced driver assistance system in a motor
27 vehicle. As used in this subdivision:

28 (i) "Advanced driver assistance system" means either of the
29 following:



1 (A) A driver support feature on a vehicle that can assist an
2 individual with steering, or braking or accelerating, but not both
3 simultaneously.

4 (B) A driver support feature on a vehicle that can control
5 both steering, and braking or accelerating, simultaneously, under
6 certain circumstances.

7 (ii) "Automated driving system" means a system, including
8 hardware and software, that is collectively capable of performing
9 the entire dynamic driving task on a sustained basis, regardless of
10 whether the system is limited to a specific operational design
11 domain, and regardless of the presence of a safety operator.

12 (r) Personal data collected and used in accordance with
13 section 830 of the controlled substances act, 21 USC 830.

14 (s) Information that is included in a limited data set as
15 described under 45 CFR 164.514(e) to the extent that the
16 information is used, disclosed, and maintained in the manner
17 prescribed under 45 CFR 164.514(e).

18 (4) A controller or processor that complies with the
19 verifiable parental consent requirements of the children's online
20 privacy protection act of 1998, 15 USC 6501 to 6506, and the rules,
21 regulations, guidance, and exemptions promulgated under that act,
22 satisfies any obligation to obtain parental consent under this act.

23 Sec. 13. (1) Except as otherwise provided in this act, a
24 consumer has all of the following rights:

25 (a) To confirm whether or not the controller is processing the
26 consumer's personal data and to access the personal data.

27 (b) To correct inaccuracies in the consumer's personal data,
28 taking into account the nature of the personal data and the
29 purposes of the processing of the consumer's personal data.



1 (c) Except as otherwise provided in section 15(8), to delete
2 personal data provided by or obtained about the consumer.

3 (d) To obtain a copy of the consumer's personal data that the
4 consumer previously provided to the controller in a portable and,
5 to the extent technically feasible, readily usable format that
6 allows the consumer to transmit the data to another controller
7 without hindrance, where the processing is carried out by automated
8 means.

9 (e) To opt out of the processing of the personal data for any
10 of the following purposes:

11 (i) Targeted advertising.

12 (ii) The sale of personal data.

13 (iii) Profiling in furtherance of solely automated decisions
14 that produce legal or similarly significant effects concerning the
15 consumer.

16 (2) A consumer may invoke the consumer rights under this
17 section at any time by submitting a request to a controller
18 specifying the consumer rights that the consumer wishes to invoke.

19 (3) If a consumer is a known child, the child's parent or
20 legal guardian may invoke the consumer rights and submit a request
21 under this section on behalf of the child.

22 (4) A consumer may also designate another person to serve as
23 the consumer's authorized agent, and act on the consumer's behalf,
24 to opt out of the processing of the consumer's personal data under
25 subsection (1)(e) by submitting a request under this section.

26 (5) A consumer may designate an authorized agent under
27 subsection (4) by any means, including, but not limited to, using
28 an internet link, a browser setting, browser extension, or global
29 device setting, in accordance with the criteria set forth in



1 section 14, indicating the consumer's intent to opt out of the
2 processing for the purposes of targeted advertising or the sale of
3 the consumer's personal data.

4 (6) A controller shall establish 1 or more secure and reliable
5 means for the submission of a request under this section.

6 (7) The secure and reliable means described in subsection (6)
7 must take into account all of the following:

8 (a) The ways in which a consumer normally interacts with the
9 controller.

10 (b) The need for secure and reliable communication of requests
11 to exercise the consumer rights under this section.

12 (c) The ability of the controller to authenticate the identity
13 of the person submitting the request under this section.

14 (8) A controller shall not require a consumer, or person on
15 behalf of the consumer under subsection (3) or (4), to create a new
16 account to submit a request under this section but may require the
17 requestor to use an existing account.

18 (9) Except as otherwise provided in this act, a controller
19 shall comply with a request submitted under this section. A
20 controller shall comply with an opt-out request received from an
21 authorized agent under subsection (4) if the controller is able to
22 verify, with commercially reasonable effort, the identity of the
23 consumer and the authorized agent's authority to act on the
24 consumer's behalf.

25 (10) A controller is not required to comply with a request
26 under subsection (1)(a) or (d), if the request would require the
27 controller to reveal a trade secret.

28 Sec. 14. (1) A controller shall allow a consumer to opt out of
29 any processing of the consumer's personal data for the purposes of



1 targeted advertising or the sale of the consumer's personal data
2 through an opt-out preference signal sent, with the consumer's
3 consent, by a platform, technology, or mechanism to the controller
4 indicating the consumer's intent to opt out of the processing or
5 sale. The platform, technology, or mechanism must do all of the
6 following:

7 (a) Not unfairly disadvantage another controller.

8 (b) Not make an opt-out preference the default setting.

9 (c) Require the consumer to make an affirmative, freely given,
10 and unambiguous choice to opt out of the processing of the
11 consumer's personal data.

12 (d) Be consumer-friendly and easy to use by the average
13 consumer.

14 (e) Be consistent with other similar platforms, technologies,
15 or mechanisms required by federal or state law or regulation.

16 (f) Enable the controller to accurately determine whether the
17 consumer is a resident of this state and whether the consumer has
18 made a legitimate request to opt out of a sale of the consumer's
19 personal data or target advertising.

20 (2) If a consumer's opt-out request is exercised through the
21 platform, technology, or mechanism under subsection (1), and the
22 request conflicts with the consumer's existing controller-specific
23 privacy setting or voluntary participation in a controller's bona
24 fide loyalty, rewards, premium features, discounts, or club card
25 program, the controller must comply with the consumer's opt-out
26 preference signal but may also notify the consumer of the conflict
27 and provide the consumer with a choice to confirm the controller-
28 specific privacy setting or participation in the controller's
29 program.



1 (3) The platform, technology, or mechanism under subsection
2 (1) is subject to the requirements of sections 13 and 15.

3 Sec. 15. (1) A controller shall respond to a request under
4 section 13 without undue delay, but in all cases not more than 45
5 days after receipt of the request.

6 (2) The response period described in subsection (1) may be
7 extended once by 45 additional days when reasonably necessary,
8 taking into account the complexity and number of the requests, if
9 the controller informs the requestor of the extension within the
10 initial 45-day response period, together with the reason for the
11 extension.

12 (3) If a controller declines to take action regarding a
13 request under section 13, the controller must inform the requestor
14 without undue delay, but in all cases and at the latest not more
15 than 45 days after receipt of the request, of the justification for
16 declining to take action and instructions for how to appeal the
17 decision under section 17.

18 (4) Any information provided in response to a request under
19 section 13 must be provided by a controller free of charge, up to
20 twice annually per consumer.

21 (5) If a request from a consumer, or on behalf of a consumer,
22 under section 13, is manifestly unfounded, excessive, or
23 repetitive, the controller may charge the requestor a reasonable
24 fee to cover the administrative costs of complying with the request
25 or decline to act on the request.

26 (6) The controller bears the burden of demonstrating that a
27 request is manifestly unfounded, excessive, or repetitive under
28 subsection (5).

29 (7) If a controller is unable to authenticate a request under



1 section 13 using commercially reasonable efforts, the controller is
2 not required to comply with the request and may ask a requestor to
3 provide additional information that is reasonably necessary to
4 authenticate the requestor and the request. A controller is not
5 required to authenticate an opt-out request, but a controller may
6 deny an opt-out request if the controller has a good faith,
7 reasonable, and documented belief that the opt-out request is
8 fraudulent. If a controller denies an opt-out request because the
9 controller believes the request is fraudulent, the controller must
10 inform the requestor without undue delay that the request was
11 denied due to the controller's belief that the request was
12 fraudulent and provide the controller's basis for that belief.

13 (8) A controller that obtains personal data about a consumer
14 from a source other than the consumer complies with a request to
15 delete personal data under section 13(1)(c) if the controller acts
16 in accordance with either of the following:

17 (a) The controller retains a record of the request, retains
18 the minimum data necessary to ensure that the consumer's personal
19 data remains deleted from the controller's records, and does not
20 use the retained data for any other purpose authorized under this
21 act.

22 (b) The controller opts the consumer out of the controller's
23 processing of the consumer's personal data for any purpose other
24 than a purpose that is exempt under this act.

25 Sec. 17. (1) A controller shall establish a process for a
26 consumer to appeal the controller's refusal to take action on a
27 request within a reasonable period of time after the consumer's
28 receipt of the decision under section 15.

29 (2) The appeal process described in subsection (1) must be



1 conspicuously available and similar to the process for submitting
2 requests to initiate action under section 13.

3 (3) Not more than 60 days after the receipt of an appeal under
4 this section, a controller shall inform the consumer in writing of
5 any action taken or not taken in response to the appeal, including
6 a written explanation of the reasons for the decisions.

7 (4) If an appeal is denied under this section, the controller
8 must provide the consumer with an online mechanism, if available,
9 or other method through which the consumer may contact the attorney
10 general to submit a complaint.

11 Sec. 19. A controller shall do all of the following:

12 (a) Except as otherwise provided in section 21(1)(c), before
13 processing any sensitive data concerning a consumer, obtain the
14 consumer's consent to process the sensitive data.

15 (b) Provide an effective mechanism for a consumer to revoke
16 the consumer's consent to process personal data that is at least as
17 easy to use as the mechanism used by the consumer to provide the
18 consumer's original consent to process personal data.

19 (c) If consent to process personal data is revoked by the
20 consumer, cease to process data as soon as practicable, but not
21 later than 15 days, after the revocation of the consent.

22 (d) If the personal data concerns a known child, process that
23 data in accordance with the children's online privacy protection
24 act of 1998, 15 USC 6501 to 6506.

25 (e) Except as otherwise provided in section 21(1)(c), limit
26 the collection of personal data to what is reasonably necessary and
27 proportionate to provide or maintain a product or service requested
28 by the consumer to whom the data pertains, and consistent with the
29 consumer's reasonable expectations, unless the personal data is



1 sensitive data, in which case the controller must limit the
2 collection of the sensitive data to what is strictly necessary to
3 provide or maintain a specific product or service requested by the
4 consumer to whom the data pertains.

5 (f) Except as otherwise provided in subdivision (g), at or
6 before the point of collecting personal data, direct the consumer
7 to the privacy notice that discloses to the consumer the purpose
8 for which the personal data will be processed.

9 (g) If the controller determines that collected data will be
10 processed for a purpose other than what was initially disclosed to
11 the consumer under subdivision (f), disclose to the consumer the
12 additional purpose for which the data will be processed and obtain
13 the consumer's consent to process the data for that additional
14 purpose.

15 (h) Establish, implement, and maintain technical and
16 organizational measures to protect the confidentiality, integrity,
17 and accessibility of personal data, which must be appropriate to
18 the volume and nature of the personal data at issue.

19 (i) Subject to the limitations and exemptions provided under
20 this act, permanently and completely delete personal data in
21 response to a consumer's request to delete that information unless
22 retention of the personal data is required by law. If a controller
23 stores any personal data on an archived or back-up system, a delay
24 in compliance with a consumer's deletion request under this
25 subparagraph may occur until the archived or back-up system is
26 restored to an active system or is next accessed or used.

27 (j) If a consumer, or a person on behalf of the consumer, has
28 opted out of the processing of the consumer's personal data under
29 section 13 or section 14, notify any processor or third party to



1 which the controller sold or otherwise disclosed the consumer's
2 personal data that the consumer has opted out of the processing of
3 the consumer's personal data.

4 Sec. 21. (1) A controller shall not do any of the following:

5 (a) Retain personal data in a form that permits identification
6 of the consumer for longer than the period that is reasonably
7 necessary for the purposes for which the personal data is processed
8 unless retention is otherwise required by law or allowed under
9 section 33.

10 (b) Retain sensitive data in a form that permits
11 identification of the consumer for longer than the period that is
12 strictly necessary for the purpose for which the sensitive data is
13 processed unless retention is otherwise required by law or under
14 section 33.

15 (c) If the controller knows or should have known that the
16 consumer is less than 18 years of age, do either of the following:

17 (i) Process the consumer's personal data for the purpose of
18 targeted advertising.

19 (ii) Sell the consumer's personal data.

20 (d) Except as otherwise provided in subsection (2), collect,
21 process, or transfer personal data in a manner that discriminates
22 against an individual or otherwise denies an individual the full
23 and equal enjoyment of goods or services because of religion,
24 actual or perceived race, color, national origin, ancestry, sex,
25 sexual orientation, gender identity, or physical or mental
26 disability.

27 (e) Subject to subsection (3), discriminate against a consumer
28 for submitting a request under section 13, including denying goods
29 or services, charging different prices or rates for goods or



1 services, or providing a different level of quality of goods and
2 services to the consumer.

3 (f) Sell the consumer's sensitive data.

4 (2) Subsection (1)(d) does not apply to either of the
5 following:

6 (a) The collection, processing, or transfer of personal data
7 for the purpose of either or the following:

8 (i) A controller's self-testing to prevent or mitigate unlawful
9 discrimination.

10 (ii) The diversification of an applicant, participant, or
11 customer pool.

12 (b) A private establishment as described in 42 USC 2000a(e).

13 (3) Subsection (1)(e) does not require a controller to provide
14 a product or service that requires the personal data of a consumer
15 that the controller does not collect or maintain or prohibits a
16 controller from offering a different price, rate, level, quality,
17 or selection of goods or services to a consumer, including offering
18 goods or services for no fee, if the offer is reasonably related to
19 a consumer's voluntary participation in a bona fide loyalty,
20 rewards, premium features, discounts, or club card program and the
21 benefit to the consumer is proportional to the benefit received by
22 the controller in collecting personal information from the reward,
23 feature, discount, or program.

24 Sec. 23. A provision of a contract or agreement of any kind
25 that purports to waive or limit in any way the consumer rights
26 under section 13 is contrary to public policy and is void and
27 unenforceable.

28 Sec. 25. (1) A controller shall provide a consumer with a
29 reasonably accessible, clear, and meaningful privacy notice that



1 includes all of the following:

2 (a) The categories of personal data processed by the
3 controller.

4 (b) The purpose for processing personal data.

5 (c) A list of the consumer rights under section 13 and section
6 14.

7 (d) A summary of how the consumer may exercise the consumer
8 rights under section 13, including, but not limited to, a
9 description of the secure and reliable means established under
10 section 13 and a summary of how the consumer may appeal a
11 controller's decision with regard to the request under section 17.

12 (e) The categories of personal data that the controller sells
13 to third parties, if any.

14 (f) The categories of third parties, if any, to whom the
15 controller sells personal data.

16 (g) If applicable, that a controller or processor uses
17 personal data to conduct internal research to develop, improve, or
18 repair products, services, or technology, if the controller or
19 processor conducting that research obtains consent from the
20 consumer and maintains the same security measures as otherwise
21 required for that personal data.

22 (h) The contact information of the controller, including an
23 active email address or other online mechanism that the consumer
24 may use to contact the controller.

25 (i) The length of time the controller intends to retain each
26 category of personal data, or, if that is impossible to determine,
27 the criteria used by the controller to determine the length of time
28 that the controller intends to retain each category of personal
29 data.



1 (j) If a controller engages in profiling in furtherance of
2 decisions that produce legal or similarly significant effects
3 concerning a consumer, a disclosure of that fact and all of the
4 following:

5 (i) A summary of how the profiling is used in the decision-
6 making process.

7 (ii) The benefits and potential consequences of the decision
8 concerning the consumer.

9 (k) The date that the privacy notice was last updated by the
10 controller.

11 (l) If the controller sells personal data to third parties,
12 processes personal data for targeted advertising, or engages in
13 profiling in furtherance of decisions that produce legal or
14 similarly significant effects concerning the consumer, the
15 controller shall disclose the sale, processing, or profiling in the
16 privacy notice and provide access to a clear and conspicuous method
17 outside the privacy notice for a consumer to opt out of the sale,
18 processing, or profiling.

19 (2) A controller shall make its privacy notice available to
20 the public in each language that the controller does either of the
21 following:

22 (a) Provides a product or service that is subject to the
23 privacy notice.

24 (b) Carries out activities related to the product or service.

25 (3) A controller shall ensure that its privacy notice can be
26 accessed and used by individuals with disabilities.

27 (4) If a controller does not have a website, the controller
28 must make its privacy notice available through a medium regularly
29 used by the controller to interact with consumers.



1 (5) If a controller makes a material change of its privacy
2 notice, the controller must make a reasonable effort to directly
3 notify each consumer affected by the material change before
4 implementing the material change, and if the material change
5 relates to the collection, processing, or sale of personal data,
6 ensure compliance with sections 19 and 21. As used in this
7 subsection, "reasonable effort" means attempting to contact a
8 consumer through a medium regularly used by the controller to
9 interact with customers, including, but not limited to, physically
10 or electronically mailing a copy of the change of its privacy
11 notice to the consumer if the controller has the consumer's
12 address.

13 (6) A controller is not required to provide a separate privacy
14 notice applicable to this state if the controller's privacy notice
15 otherwise complies with this section.

16 Sec. 27. (1) A processor shall adhere to the instructions of a
17 controller and shall assist the controller in meeting the
18 controller's obligations under this act. The assistance provided by
19 a processor to a controller must include all of the following:

20 (a) Assistance in fulfilling the controller's obligation to
21 respond to requests submitted under section 13, taking into account
22 the nature of processing and the information available to the
23 processor, by appropriate technical and organizational measures, to
24 the extent reasonably practicable.

25 (b) Assisting the controller in meeting obligations in
26 relation to the security and processing of personal data and to the
27 notification of a security breach under the identity theft
28 protection act, 2004 PA 452, MCL 445.61 to 445.79d, taking into
29 account the nature of processing and the information available to



1 the processor.

2 (c) Providing necessary information to enable the controller
3 to conduct and document data protection impact assessments under
4 section 29.

5 (2) A contract between a controller and a processor must
6 govern the processor's data processing procedures with respect to
7 processing performed on behalf of the controller. The contract must
8 be binding and clearly set forth instructions for processing data,
9 the nature and purpose of processing, the type of data subject to
10 processing, the duration of processing, and the rights and
11 obligations of both parties. The contract must include requirements
12 that the processor do all of the following:

13 (a) Ensure that each person processing personal data is
14 subject to a duty of confidentiality with respect to the data.

15 (b) At the controller's direction, delete or return all
16 personal data to the controller as requested at the end of the
17 provision of services, unless retention of the personal data is
18 required by law.

19 (c) On the reasonable request of the controller, make
20 available to the controller all information in its possession
21 necessary to demonstrate the processor's compliance with the
22 obligations in this act.

23 (d) Either of the following:

24 (i) Allow, and cooperate with, reasonable assessments by the
25 controller or the controller's designated assessor of the
26 processor's policies and technical and organizational measures in
27 support of the obligations under this act.

28 (ii) Arrange for a qualified and independent assessor to
29 conduct an assessment of the processor's policies and technical and



1 organizational measures in support of the obligations under this
 2 act using an appropriate and accepted control standard or framework
 3 and assessment procedure for those assessments. The processor shall
 4 provide a report of the assessment to the controller on request.

5 (e) Engage any subprocessor under a written contract that
 6 requires the subprocessor to meet the obligations of the processor
 7 with respect to the personal data.

8 (f) Require the processor to notify the controller of its
 9 engagement with any subprocessor.

10 (3) This section does not relieve a controller or a processor
 11 from the liabilities imposed on it by virtue of its role in the
 12 processing relationship under this act.

13 (4) Determining whether a person is acting as a controller or
 14 processor with respect to a specific processing of data is a fact-
 15 based determination that depends on the context in which personal
 16 data is to be processed. A processor that continues to adhere to a
 17 controller's instructions with respect to a specific processing of
 18 personal data remains a processor.

19 Sec. 29. (1) A controller shall conduct and document a data
 20 protection impact assessment of each of the following processing
 21 activities involving personal data:

22 (a) The processing of personal data for purposes of targeted
 23 advertising.

24 (b) The sale of personal data.

25 (c) The processing of personal data for the purpose of
 26 profiling, if the profiling presents a reasonably foreseeable risk
 27 of any of the following:

28 (i) Unfair or deceptive treatment of, or unlawful disparate
 29 impact on, consumers.



1 (ii) Financial, physical, or reputational injury to consumers.

2 (iii) A physical or other intrusion on the solitude or
3 seclusion, or the private affairs or concerns, of consumers where
4 the intrusion would be offensive to a reasonable person.

5 (iv) Other substantial injury to consumers.

6 (d) The processing of sensitive data.

7 (e) Any processing activities involving personal data that
8 present a heightened risk of harm to consumers.

9 (2) A data protection impact assessment conducted under
10 subsection (1) must identify and weigh the benefits that may flow,
11 directly and indirectly, from the processing to the controller, the
12 consumer, other stakeholders, and the public against the potential
13 risks to the rights of the consumer associated with the processing,
14 as mitigated by safeguards that can be employed by the controller
15 to reduce those risks. The use of de-identified data and the
16 reasonable expectations of consumers, as well as the context of the
17 processing and the relationship between the controller and the
18 consumer whose personal data will be processed, must be factored
19 into the assessment by the controller.

20 (3) Subject to section 39, the attorney general may request
21 that a controller disclose any data protection impact assessment
22 that is relevant to an investigation conducted by the attorney
23 general, and the controller must make the data protection impact
24 assessment available to the attorney general. The attorney general
25 may evaluate the data protection impact assessment for compliance
26 with the responsibilities set forth in sections 13 to 21. A data
27 protection impact assessment is confidential and exempt from public
28 inspection and copying under the freedom of information act, 1976
29 PA 442, MCL 15.231 to 15.246. The disclosure of a data protection



1 impact assessment in accordance with a request from the attorney
2 general does not constitute a waiver of attorney-client privilege
3 or work product protection with respect to the assessment and any
4 information contained in the assessment.

5 (4) A single data protection impact assessment may address a
6 comparable set of processing operations that include similar
7 activities.

8 (5) A data protection impact assessment conducted by a
9 controller for the purpose of complying with other laws or
10 regulations may satisfy the requirements of this section if the
11 assessment has a reasonably comparable scope and effect.

12 (6) The data protection impact assessment requirements of this
13 section apply to processing activities created or generated after
14 the effective date of this act and are not retroactive.

15 Sec. 31. (1) A controller in possession of de-identified data
16 shall do all of the following:

17 (a) Take reasonable measures to ensure that the data cannot be
18 associated with an individual.

19 (b) Publicly commit to maintaining and using de-identified
20 data without attempting to re-identify the data.

21 (c) Contractually obligate any recipients of the de-identified
22 data to comply with all provisions of this act.

23 (2) This act does not require a controller or processor to re-
24 identify de-identified data or pseudonymous data or maintain data
25 in identifiable form, or collect, obtain, retain, or access any
26 data or technology, to be capable of associating an authenticated
27 request under section 13 with personal data.

28 (3) A controller or processor is not required to comply with
29 an authenticated request under section 13 if all of the following



1 apply:

2 (a) The controller is not reasonably capable of associating
3 the request with personal data of the requesting consumer or it
4 would be unreasonably burdensome for the controller to associate
5 the request with personal data.

6 (b) The controller does not use the personal data to recognize
7 or respond to the specific consumer who is the subject of the
8 personal data, or associate the personal data with other personal
9 data about the same specific consumer.

10 (c) The controller does not sell the personal data to any
11 third party or otherwise voluntarily disclose the personal data to
12 any third party other than a processor, except as otherwise
13 permitted in this section.

14 (4) The consumer rights described in section 13(1)(a) to (d)
15 do not apply to pseudonymous data if the controller is able to
16 demonstrate that any information necessary to identify the consumer
17 is kept separately and is subject to effective technical and
18 organizational measures that prevent the controller from accessing
19 the information.

20 (5) A controller that discloses pseudonymous data or de-
21 identified data shall exercise reasonable oversight to monitor
22 compliance with any contractual commitments to which the
23 pseudonymous data or de-identified data is subject and shall take
24 appropriate steps to address any breaches of those contractual
25 commitments.

26 Sec. 33. (1) This act does not restrict a controller's or
27 processor's ability to do any of the following:

28 (a) Comply with federal, state, or local laws, rules, or
29 regulations.



1 (b) Comply with a civil, criminal, or regulatory inquiry,
2 investigation, subpoena, or summons by federal, state, local, or
3 other governmental authorities.

4 (c) Cooperate with a law enforcement agency concerning conduct
5 or activity that the controller or processor reasonably and in good
6 faith believes may violate federal, state, or local laws, rules, or
7 regulations.

8 (d) Investigate, establish, exercise, prepare for, or defend
9 legal claims.

10 (e) Provide a product or service specifically requested by a
11 consumer, perform a contract to which the consumer is a party,
12 including fulfilling the terms of a written warranty, or take steps
13 at the request of the consumer before entering into a contract.

14 (f) Take immediate steps to protect an interest that is
15 essential for the life or physical safety of the consumer or
16 another individual, and where the processing cannot be manifestly
17 based on another legal basis.

18 (g) Prevent, detect, protect against, or respond to security
19 incidents, identity theft, fraud, harassment, malicious or
20 deceptive activities, or any illegal activity; preserve the
21 integrity or security of systems; or investigate, report, or
22 prosecute those responsible for any activity described in this
23 subdivision.

24 (h) Engage in public or peer-reviewed scientific or
25 statistical research in the public interest that adheres to all
26 other applicable ethics and privacy laws and is approved,
27 monitored, and governed by an institutional review board or similar
28 independent oversight entities that determine all of the following:

29 (i) If the deletion of the information is likely to provide



1 substantial benefits that do not exclusively accrue to the
2 controller.

3 (ii) If the expected benefits of the research outweigh the
4 privacy risks.

5 (iii) If the controller has implemented reasonable safeguards to
6 mitigate privacy risks associated with research, including any
7 risks associated with re-identification.

8 (i) Assist another controller, processor, or third party with
9 any of the obligations under this section.

10 (2) An obligation imposed on a controller or processor under
11 this act does not restrict the controller's or processor's ability
12 to collect, use, or retain data to do any of the following:

13 (a) Conduct internal research to develop, improve, or repair
14 products, services, or technology if the controller or processor
15 conducting that research obtains consent from the consumer and
16 maintains the same security measures as otherwise required for that
17 personal data.

18 (b) Effectuate a product recall.

19 (c) Identify and repair a technical error that impairs
20 existing or intended functionality.

21 (d) Perform an internal operation that is reasonably aligned
22 with an expectation of a consumer or reasonably anticipated based
23 on the consumer's existing relationship with the controller or is
24 otherwise compatible with processing data in furtherance of the
25 provision of a product or service specifically requested by a
26 consumer or the performance of a contract to which the consumer is
27 a party.

28 (3) A requirement imposed under this act does not apply if
29 compliance by a controller or processor with that requirement would



1 violate an evidentiary privilege under the laws of this state. This
2 act does not prevent a controller or processor from providing a
3 consumer's personal data to a person covered by an evidentiary
4 privilege under the laws of this state as part of a privileged
5 communication.

6 (4) A controller or processor that discloses personal data to
7 a third-party controller or processor in compliance with this act
8 does not violate this act if the third-party controller or
9 processor that receives and processes the personal data violates
10 this act, if, at the time of disclosing the personal data, the
11 disclosing controller or processor did not have actual knowledge
12 that the recipient intended to commit a violation. A third-party
13 controller or processor that receives personal data from a
14 controller or processor in compliance with this act does not
15 violate this act if the controller or processor from which the
16 third-party controller or processor received the personal data
17 violated this act.

18 (5) This act does not impose an obligation on a controller or
19 processor that adversely affects the rights or freedoms of any
20 person, including, but not limited to, exercising the right of free
21 speech, or apply to the processing of personal data by a person in
22 the course of a purely personal or household activity.

23 (6) Except as otherwise provided in this act, personal data
24 processed by a controller under this section must not be processed
25 for any purpose other than those expressly listed in this section.
26 Personal data processed by a controller under this section may be
27 processed to the extent that both of the following apply to that
28 processing:

29 (a) The processing of the personal data is reasonably



1 necessary and proportionate, or if the personal data is sensitive
 2 data, is strictly necessary, to the purposes described in this
 3 section.

4 (b) The processing of the personal data is adequate, relevant,
 5 and limited to what is necessary, or if the personal data is
 6 sensitive data, strictly necessary, in relation to the specific
 7 purposes described in this section. Personal data that is
 8 collected, used, or retained under subsection (2) must, if
 9 applicable, take into account the nature and purpose of the
 10 collection, use, or retention. The personal data is subject to
 11 reasonable administrative, technical, and physical measures to
 12 protect the confidentiality, integrity, and accessibility of the
 13 personal data and to reduce reasonably foreseeable risks of harm to
 14 consumers relating to the collection, use, or retention of personal
 15 data.

16 (7) If a controller processes personal data under an exemption
 17 in this section, the controller bears the burden of demonstrating
 18 that the processing qualifies for the exemption and complies with
 19 the requirements in subsection (6).

20 (8) The processing of personal data for the purposes in
 21 subsection (1) does not solely make a person a controller with
 22 respect to that processing.

23 Sec. 35. (1) Beginning on February 1, 2026, and on each
 24 February 1 thereafter, if for the previous calendar year a person
 25 meets the definition of a data broker under this act, the person
 26 must register with the attorney general as a data broker.

27 (2) A person shall do all of the following when registering as
 28 a data broker:

29 (a) Pay a registration fee in an amount determined by the



1 attorney general, not to exceed the reasonable costs of
2 establishing and maintaining the informational website described in
3 subsection (3).

4 (b) Provide all of the following information:

5 (i) Its name.

6 (ii) Its primary physical, email, and website addresses.

7 (iii) Any additional information or explanation that it chooses
8 to provide concerning its data collection practices.

9 (3) The attorney general shall create a page on its website
10 where the information provided by data brokers under subsection (2)
11 is accessible by the public.

12 (4) The attorney general may bring a civil action under
13 section 39 against a data broker that fails to register under this
14 section.

15 (5) The registration fees received under this section must be
16 deposited in the data broker registry fund created under section
17 45.

18 Sec. 37. A person may not use a geofence to establish a
19 virtual boundary that is within 1,750 feet of any mental health
20 facility or reproductive or sexual health facility for the purpose
21 of identifying, tracking, or collecting data from or sending any
22 notification to a consumer regarding the consumer's consumer health
23 data.

24 Sec. 39. (1) Before initiating a civil action under this act,
25 if the attorney general has reasonable cause to believe that a
26 person subject to this act has engaged in, is engaging in, or is
27 about to engage in a violation of this act, the attorney general
28 may initiate an investigation and may require the person or an
29 officer, member, employee, or agent of the person to appear at a



1 time and place specified by the attorney general to give
2 information under oath and to produce books, memoranda, papers,
3 records, documents, or other relevant evidence in the possession,
4 custody, or control of the person ordered to appear.

5 (2) When requiring the attendance of a person or the
6 production of documents under subsection (1), the attorney general
7 shall issue an order setting forth the time when and the place
8 where attendance or production is required and shall serve the
9 order on the person in the manner provided for service of process
10 in civil cases not less than 5 days before the date fixed for
11 attendance or production. The order issued by the attorney general
12 has the same force and effect as a subpoena. If a person does any
13 of the following, the person may be ordered to pay a civil fine of
14 not more than \$5,000.00:

15 (a) Knowingly, without good cause, fails to appear when served
16 with an order of the attorney general under this section.

17 (b) Knowingly avoids, evades, or prevents compliance, in whole
18 or in part, with an investigation under this section, including the
19 removal from any place, concealment, destruction, mutilation,
20 alternation, or falsification of documentary material in the
21 possession, custody, or control of the person subject to an order
22 of the attorney general under this section.

23 (c) Knowingly conceals information that is relevant to the
24 attorney general's investigation under this section.

25 (3) On application of the attorney general, an order issued by
26 the attorney general under subsection (2), may be enforced by a
27 court having jurisdiction over the person, Ingham County circuit
28 court, or the circuit court of the county where the person
29 receiving the order resides or is found in the same manner as



1 though the notice were a subpoena. If a person fails or refuses to
2 obey the order issued by the attorney general under subsection (2),
3 the court may issue an order requiring the person to appear before
4 the court, to produce documentary evidence, or to give testimony
5 concerning the matter in question. A failure to obey the order of
6 the court is punishable by that court as contempt.

7 (4) Subject to subsections (5) and (6), if a person violates
8 this act, the attorney general may bring a civil action seeking 1
9 or more of the following:

10 (a) If the violation is not a violation of section 35, a civil
11 fine of not more than \$7,500.00 for each violation.

12 (b) If the violation is a violation of section 35, 1 or more
13 of the following:

14 (i) A civil fine of \$100.00 for each day the data broker fails
15 to register under section 35.

16 (ii) An amount equal to the registration fees that were due
17 during the period the data broker failed to register under section
18 35.

19 (c) Expenses incurred by the attorney general in the
20 investigation and prosecution of the civil action, including, but
21 not limited to, attorney fees, as the court considers appropriate.

22 (d) Injunctive or declaratory relief.

23 (e) Any other relief the court considers appropriate.

24 (5) Except as otherwise provided in subsection (6), the
25 attorney general shall not initiate an action under this section
26 unless the attorney general provides notice as required under
27 subdivision (a) and subdivision (b) does not apply:

28 (a) Before initiating an action under this section, the
29 attorney general shall provide a person that the attorney general



1 alleges has been or is violating this act 30 days' written notice
2 identifying the specific provisions of this act the attorney
3 general alleges have been or are being violated.

4 (b) If, within 30 days of receiving the notice under
5 subdivision (a), the person cures the noticed violations and
6 provides the attorney general with an express written statement
7 that the violations have been cured and further such violations
8 will not occur, the attorney general must not initiate a civil
9 action against the person under this section. The right to cure
10 under this subdivision exists for a period of 18 months following
11 the effective date of this act.

12 (6) If a person continues to violate this act in breach of the
13 express written statement under subsection (5) or if the person
14 fails to cure a violation within 30 days after being notified of
15 the alleged noncompliance in accordance with subsection (5), the
16 attorney general may initiate a civil action under this section.

17 (7) A default in the payment of a civil fine or costs ordered
18 under this act or an installment of the fine or costs may be
19 remedied by any means authorized under chapter 40 or 60 of the
20 revised judicature act of 1961, 1961 PA 236, MCL 600.4001 to
21 600.4065 and 600.6001 to 600.6098.

22 (8) A civil fine or expense collected under this section must
23 be deposited in the consumer privacy fund created in section 43.

24 (9) The registration fees collected under this section must be
25 deposited in the data broker registry fund created under section
26 45.

27 (10) If the attorney general commences a civil action under
28 this act, the attorney general's filing fees for that action must
29 be waived.



1 (11) The attorney general has the exclusive authority to
2 enforce this act. There is no private right of action under this
3 act.

4 Sec. 43. (1) The consumer privacy fund is created within the
5 state treasury.

6 (2) The state treasurer may receive money or other assets from
7 any source for deposit into the fund. The state treasurer shall
8 direct the investment of the fund. The state treasurer shall credit
9 to the fund interest and earnings from fund investments.

10 (3) Money in the fund at the close of the fiscal year remains
11 in the fund and does not lapse to the general fund.

12 (4) The department of attorney general is the administrator of
13 the fund for auditing purposes.

14 (5) The department of attorney general shall expend money from
15 the fund, subject to appropriation, to enforce the provisions of
16 this act and to offset costs incurred by the attorney general in
17 connection with this act.

18 (6) As used in this section, "fund" means the consumer privacy
19 fund created under subsection (1).

20 Sec. 45. (1) The data broker registry fund is created within
21 the state treasury.

22 (2) The state treasurer may receive money or other assets from
23 any source for deposit into the fund. The state treasurer shall
24 direct the investment of the fund. The state treasurer shall credit
25 to the fund interest and earnings from fund investments.

26 (3) Money in the fund at the close of the fiscal year remains
27 in the fund and does not lapse to the general fund.

28 (4) The department of attorney general is the administrator of
29 the fund for auditing purposes.



1 (5) The department of attorney general shall expend money from
2 the fund, subject to appropriation, to provide all of the following
3 information on the website described under section 35:

4 (a) The name of the data broker and its primary physical,
5 email, and website addresses.

6 (b) Any additional information or explanation that the data
7 broker chooses to provide concerning its data collection practices.

8 (6) As used in this section, "fund" means the data broker
9 registry fund created under subsection (1).

10 Enacting section 1. This act takes effect 1 year after the
11 date it is enacted into law.

