As Introduced

134th General Assembly
Regular Session
2021-2022

Representatives Carfagna, Hall
Cosponsors: Representatives Click, Plummer, Schmidt, Lanese, White, Stewart, Carruthers, Ginter

A BILL

To enact sections 1355.01, 1355.02, 1355.03, 1355.04, 1355.05, 1355.06, 1355.07, 1355.08, and 1355.09 of the Revised Code to enact the Ohio Personal Privacy Act.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF OHIO:

Section 1. That sections 1355.01, 1355.02, 1355.03, 1355.04, 1355.05, 1355.06, 1355.07, 1355.08, and 1355.09 of the Revised Code be enacted to read as follows:

Sec. 1355.01. As used in this chapter:

(A)(1) "Affiliate" means a legal entity that controls, is controlled by, shares common branding with, or is under common control with, another legal entity.

(2) For purposes of division (A)(1) of this section, "control" or "controlled" means a relationship between two legal entities characterized by any of the following:

(a) One entity having ownership of, or the power to vote, more than fifty per cent of the outstanding shares of any class
of voting security of the other legal entity;

(b) One entity having control in any manner over the election of a majority of the directors, or of individuals exercising similar functions, of the other entity;

(c) One entity having the power to exercise a controlling influence over the management of the other entity.

(B) "Aggregated data" means personal data that has been aggregated using commercially reasonable methods such that a consumer cannot be reasonably identified.

(C) "Business" means any limited liability company, limited liability partnership, corporation, sole proprietorship, association, or other group, however organized and regardless of whether operating for profit or not for profit, including a financial institution organized, chartered, or holding a license authorizing operation under the laws of this state, any other state, the United States, or any other country, or the parent or subsidiary of any of the foregoing. "Business" does not include a public entity, including a political subdivision of this state, a city, township, or a county.

(D) "Child" means any natural person under thirteen years of age.

(E) "Commercial purpose" means the processing of information for the purpose of obtaining any form of consideration from either of the following:

(1) The person that is the subject of such information;

(2) Any third party.

(F) "Consent" means a clear affirmative act signifying a freely given, specific, informed, and unambiguous indication of
a consumer's agreement to the processing of personal data relating to the consumer, such as by a written statement, including by electronic means, or other course of action that would clearly indicate that consent has been provided.

(G) "Consumer" means a natural person who is a resident of this state acting only in an individual or household context. "Consumer" does not include a natural person acting in a business capacity or employment context, including contractors, job applicants, officers, directors, or owners.

(H) "Deidentified data" means personal data that has been deidentified using commercially reasonable methods such that a consumer, or a device linked to a consumer, cannot be reasonably identified.

(I) "HIPAA" has the same meaning as in section 3965.01 of the Revised Code.

(J) "Personal data" means any information that relates to an identified or identifiable consumer processed by a business for a commercial purpose. "Personal data" does not include either of the following:

(1) Any such data processed from publicly available sources;

(2) Pseudonymized, deidentified, or aggregate data.

(K) "Process" or "processing" means any operation or set of operations that are performed on personal data, whether or not by automated means, including the collection, use, storage, disclosure, analysis, deletion, transfer, or modification of personal data.

(L) "Processor" means a natural or legal person who
processes personal data on behalf of a business subject to this chapter.

(M) "Pseudonymized or pseudonymous data" means information that no longer allows the identification of an individual without combining it with other information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable consumer.

(N) "Publicly available information" means information that is lawfully made available from federal, state, or local government records. "Publicly available information" includes widely available media.

(O)(1) "Sale," "sell," or "sold" means the exchange of personal data for monetary or other valuable consideration by a business to a third party.

(2) "Sale," "sell," or "sold" does not include any of the following:

(a) The disclosure of personal data to a processor who processes the personal data on behalf of a business;

(b) The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;

(c) The disclosure of personal data from one business to another business without monetary or other valuable consideration;

(d) The disclosure or transfer of personal data to an affiliate of the business;
(e) The disclosure of information that a consumer intentionally made available to the general public via a channel of mass media and did not restrict to a specific audience;

(f) The disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business's assets, so long as the third party agrees to treat the data in accordance with the representations made in selling business's privacy policy or if the third party obtains affirmative consent from consumers to the third party's current privacy policy.

(P) "Third party" means a natural or legal person, public authority, agency, or body other than the consumer, business, or processor, or an affiliate of the business or processor.

(Q) "Verified request" means a request submitted to a business under sections 1355.03 to 1355.06 of the Revised Code that has been verified by the business as being made by the consumer in question or by the consumer's representative.

As used in division (Q) of this section, "consumer's representative" includes a child's parent or a representative of a person for whom a guardian of the estate or conservator has been appointed.

Sec. 1355.02. (A) This chapter applies to businesses that conduct business in this state, or produce products or services targeted to consumers in this state, that satisfy one or more of the following criteria:

(1) The business's annual gross revenues generated in this state exceed twenty-five million dollars;

(2) During a calendar year, the business controls or
processes personal data of one hundred thousand or more consumers;

(3) During a calendar year, the business derives over fifty per cent of its gross revenue from the sale of personal data and processes or controls personal data of twenty-five thousand or more consumers.

(B) This chapter does not apply to any of the following:

(1) Any body, authority, board, bureau, commission, district, or agency of this state or of any political subdivision of this state;

(2) A financial institution, data, or an affiliate of a financial institution governed by Title V of the federal "Gramm-Leach-Bliley Act," 15 U.S.C. 6801 et seq. and related regulations;

(3) A covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States department of health and human services, 45 C.F.R. Parts 160 and 164 established pursuant to HIPAA, and the health information technology for economic and clinical health act, 42 U.S.C. 300jj et seq;

(4) An institution of higher education.

(5) Business to business transactions.

(6) Any of the following:

(a) Any insurer or independent insurance agent, as defined in section 3905.49 of the Revised Code;

(b) Any nonprofit organization established to detect or prevent insurance-related crime or fraud;
(c) Any advisory organization described in section 3937.09 of the Revised Code;

(d) Any rating organization licensed pursuant to section 3937.05 of the Revised Code or an affiliate thereof.

(C) The following information and data are exempt from this chapter:

(1) Protected health information under HIPAA;

(2) Health records, as described in Chapter 3798. of the Revised Code;

(3) Patient identifying information for purposes of 42 U.S.C. 290dd-2;

(4) Any of the following types of information or data:

(a) Identifiable private information for purposes of the federal policy for the protection of human subjects under 45 C.F.R. Part 46;

(b) Identifiable private information that is otherwise information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the international council for harmonisation of technical requirements for pharmaceuticals for human use;

(c) Data related to the protection of human subjects under 21 C.F.R. parts 6, 50, and 56, or personal data used or shared in research conducted in accordance with the requirements set forth in this chapter, or other research conducted in accordance with applicable law.

11101 et seq.;


(7) Information derived from any of the health care-related information listed in division (C) of this section that is deidentified in accordance with the requirements for deidentification pursuant to HIPAA;

(8) Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as information exempt under division (C) of this section that is maintained by a covered entity or business associate as defined by HIPAA or a program or a qualified service organization as defined by 42 U.S.C. 290dd-2;

(9) Information used only for public health activities and purposes as authorized by HIPAA;

(10) The collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency or furnisher that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the federal "Fair Credit Reporting Act," 15 U.S.C. 1681 et seq.;

(11) Personal data collected, processed, sold, or disclosed in compliance with the federal "Driver's Privacy Protection Act of 1994," 18 U.S.C. 2721 et seq.;

(12) Personal data regulated by the federal "Family
Educational Rights and Privacy Act," 20 U.S.C. 1232g et seq.;

(13) Personal data collected, processed, sold, or
disclosed in compliance with the federal "Farm Credit Act," 12
U.S.C. 2001 et seq.;

(14) Data processed or maintained in accordance with any of the following:

(a) In the course of an individual applying to, employed by, or acting as an agent or independent contractor of a business subject to this chapter, processor, or a related third party, to the extent that the data is collected and used within the context of that role;

(b) For emergency contact purposes for individuals described in division (C)(14)(a) of this section;

(c) As necessary to administer employment benefits to those individuals described in division (C)(14)(a) of this section, as well as to any persons related to those individuals, such as dependents or spouses.

(D) This chapter does not apply to the extent necessary for a business to do any of the following:

(1) Comply with federal or state law;

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities;

(3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law;
(4) Exercise, or defend against, legal claims;

(5) (a) Prevent, detect, or protect against, or provide a response to, security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity;

(b) Report or prosecute those responsible for any such action.

(6) Preserve the integrity or security of systems;

(7) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, if the deletion of the information is likely to render impossible or seriously impair the achievement of the research and the consumer in question has provided consent;

(8) Assist another business, processor, or third party with any of the obligations imposed under division (C) of this section.

(E) The requirements of this chapter do not apply to the extent that compliance would violate or hinder an evidentiary privilege under Ohio law.

(F) The obligations imposed on businesses or processors under this chapter shall not be construed as restricting a business's or processor's ability to collect, use, or retain data as necessary to do any of the following:

(1) Conduct internal research solely to improve or repair products, services, or technology;

(2) Identify and repair technical errors that impair existing or intended functionality;
(3) Perform solely internal operations that are reasonably aligned with the expectations of the consumer based on the consumer's existing relationship with the business, or are otherwise compatible with processing in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract or warranty to which the consumer is a party;

(4) Effectuate a product recall.

(G) This chapter shall not be construed as requiring a business to collect personal data that it would not otherwise collect in the ordinary course of its business, retain personal data for longer than it would otherwise retain such data in the ordinary course of its business, or reidentify or otherwise link information that is not maintained in a manner that would be considered personal data.

(H) Obligations imposed on businesses and processors under this chapter shall not be construed as doing either of the following:

(1) Adversely affecting the rights or freedoms of any persons, such as exercising the right of free speech pursuant to the first amendment of the United States Constitution or Article I, Section 11, of the Ohio Constitution;

(2) Applying to the processing of personal data by a natural person in the course of a purely personal or household activity.

Sec. 1355.03. (A) A consumer has a right to know the personal data that a business collects about that consumer, such as by obtaining a privacy policy from the business.

(B) A business shall provide consumers notice about the
personal data that it processes about the consumer by providing a reasonably accessible, clear, and conspicuously posted privacy policy.

(C)(1) The privacy policy shall include all of the following:

(a) The identity and the contact information of the business, including the business's contact for privacy and data security inquiries, and the identity of any affiliate to which personal data may be transferred by the business;

(b) The categories of personal data the business processes;

(c) The purposes of processing for each category of personal data;

(d) The purposes for collecting or selling personal data;

(e) The categories of sources from which the personal data is collected;

(f) The categories of processors with whom the business discloses personal data;

(g) Whether the business sells personal data, the categories of third parties to whom the business sells personal data, and the purposes of the sale;

(h) A description of the business's data retention practices for personal data and the purposes for such retention;

(i) How individuals can exercise their rights under this chapter;

(j) A general description of the business's data security practices;
(k) The effective date of the privacy policy;

(l) A description of how the business will notify consumers, pursuant to division (E) of this section, when it makes a material change to its privacy policy or decides to process personal data for purposes incompatible with the privacy policy.

(2)(a) The privacy policy shall also disclose any and all commercial purposes for which the company collects or processes personal data.

(b) Failure on the part of a business to maintain a privacy policy that reflects the business's data privacy practices to a reasonable degree of accuracy shall be considered an unfair and deceptive practice under Chapter 1345. of the Revised Code, except that a consumer shall not be entitled to a private cause of action under that chapter for a failure to comply with division (C)(2)(a) of this section.

(D) A business, a co-business, or a processor may provide the privacy policy to the consumer.

(E) If a business makes a material change to its privacy policy or decides to process personal data for purposes incompatible with the privacy policy, it shall do either of the following prior to further processing previously collected personal data:

(1) Obtain affirmative consent from the consumers affected;

(2)(a) Provide notice outlining the changes to the business's privacy policy and providing affected consumers a reasonable means to opt out of having their data processed or disseminated.
(b) Such notice shall be provided not less than sixty days prior to implementing the change, taking into account available technology and the nature of the relationship between the business and the consumer.

(F) The business shall provide direct notification, where possible, regarding a material change to the privacy policy to affected consumers, taking into account available technology and the nature of the relationship.

Sec. 1355.04. (A) A consumer has a right to request access to and the disclosure of the personal data that a business collects about that consumer by making a verifiable request to access the consumer's personal data.

(B)(1)(a) A business shall provide at least one of the following methods for consumers to make requests under this section:

(i) A toll-free telephone number;

(ii) An electronic mail address;

(iii) A web form;

(iv) A clear and conspicuous link on the business's main internet homepage to an internet web page that enables a consumer to exercise the rights provided under this section.

(b) However, if the consumer maintains an account with the business, the business may require the consumer to submit the request through that account. If the consumer does not maintain an account, the business shall not require that an account be created to submit the request.

(2) A business shall reasonably verify the identity of the consumer before providing access and disclosing data under this
section.

(3) Upon receiving a verified request, a business shall disclose both of the following to the consumer in question in conformance with this section:

(a) The categories of third parties to whom the business sells personal data, or if it does not sell personal data, that fact;

(b) The personal data the business has collected about the consumer.

(4) A business need not respond to a consumer request made under this section if the business is unable to reasonably verify the consumer.

(C) The disclosure shall cover the twelve-month period preceding the business's receipt of the request.

(D)(1) A business shall provide the requested personal data free of charge, within forty-five calendar days of the request.

(2)(a) For reasonable cause, and upon notice to the consumer citing the cause for the delay, a business may extend the time required to respond to a request under this section by an additional forty-five calendar days.

(b) Such a delay shall not be used more than one time.

(E) The consumer may request that the consumer's personal data be provided electronically in a portable, readily usable format or using paper mailed to the consumer.

(F) A business is not obligated to provide access to a consumer's personal data more than once in a twelve-month
period, beginning from the prior date on which the consumer made
a request pursuant to this section.

(G) A business may redact personal data in its responses
to consumers to protect the security of personal data,
including, without limitation, redacting social security
numbers, financial account numbers, or driver's license numbers.

Sec. 1355.05. (A) A consumer shall have the right to
request that a business delete personal data that the business
has collected from the consumer for commercial purposes and that
the business maintains in an electronic format.

(B)(1)(a) A business shall provide at least one of the
following methods for consumers to make requests under this
section:

(i) A toll-free telephone number;

(ii) An electronic mail address;

(iii) A web form;

(iv) A clear and conspicuous link on the business's main
internet homepage to an internet web page that enables a
consumer to exercise the rights provided under this section.

(b) Consumers may submit a verifiable request to delete
personal data in writing to the business. However, if a consumer
maintains an account with the business, the business may require
the consumer to submit the request through that account.

(2) Such a verifiable request shall reasonably describe
the personal data the consumer is requesting be deleted.

(3) A business need not respond to a consumer request made
under this section if the business is unable to reasonably
verify the consumer.

(4) Within forty-five calendar days after verifying the consumer's identity, a business shall either delete the personal data or notify the consumer of its refusal to make such deletion and the reason for refusal.

(C)(1) If the consumer's personal data is stored on archived or backup systems, the business may delay compliance with the consumer's request to delete until the archived or backup system relating to that data is restored to an active system, next accessed, or used for a sale, disclosure, or commercial purpose.

(2) If the consumer's personal data is stored on archived or backup systems, the business may comply with the consumer's request by deleting or overwriting the data in accordance with a scheduled backup or creation of a new archive, so long as the business employs encryption standards to protect that data both when the data is in transit and is at rest.

(D) A business is not required to delete personal data that it maintains or uses as aggregated, deidentified, or pseudonymous data, provided that such data in the possession of the business is not linked to a specific consumer.

(E) A business, or an associated processor, shall not be required to comply with a consumer's request to delete personal data if it is necessary for the business or service provider to maintain the consumer's personal data in order to do any of the following:

(1) Comply with federal, state, or local laws, rules, or regulations;

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

(3) Adhere to its written records retention schedule;

(4) Cooperate with law enforcement agencies concerning conduct or activity that the business, or service provider, reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations;

(5) Investigate, establish, exercise, prepare for, or defend legal claims;

(6) Provide a product or service specifically requested by a consumer, or reasonably anticipated within the context of the business's ongoing business relationship with the consumer, or otherwise perform a contract or warranty to which the consumer is a party, or take steps at the request of the consumer prior to entering into a contract;

(7) Take immediate steps to protect an interest that is essential for the life of the consumer or of another natural person, and where the processing cannot be manifestly based on another legal basis;

(8) Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity;

(9) Preserve the integrity or security of systems;

(10) Investigate, report, or prosecute those responsible for any such action described in divisions (E)(8) and (9) of this section;

(11) Engage, with the consent of the consumer, in public or peer-reviewed scientific, historical, or statistical research
in the public interest that adheres to all other applicable ethics and privacy laws if the deletion of the information is likely to render impossible or seriously impair the achievement of the research; 

(12) Assist another party with any of the obligations prescribed in division (E) of this section.

Sec. 1355.06. (A) A consumer has a right to request that a business that sells personal data to third parties not sell the consumer's personal data.

(B)(1) A business shall provide at least one of the following methods for consumers to make a request under this section:

(a) A toll-free telephone number;

(b) An electronic mail address;

(c) A web form;

(d) A clear and conspicuous link on the business's main internet homepage to an internet web page that enables a consumer to exercise the rights provided under this section.

(2) Upon receipt of a verified request made under division (A) of this section, a business shall not sell the personal data of the consumer in question.

(3) Verification shall be completed or, if appropriate contact information can reasonably be obtained per the consumer's request, the consumer shall be contacted to complete verification without unreasonable delay, at most within thirty calendar days.

(C) A business shall not sell the personal data of

(D) A business that sells personal data shall provide clear and conspicuous notice of this fact in such a manner as to enable a consumer to opt out of the sale of the consumer's personal data; such as by providing clear and conspicuous notice on its web site privacy policy or other publicly available notice.

(E) A business is not required to comply with an opt-out request that the business reasonably determines to be fraudulent.

(F) A business shall inform its processors or third parties of a consumer's request to opt out and request that they comply with the consumer's opt-out request.

**Sec. 1355.07.** (A) Subject to divisions (B) and (C) of this section, a business shall not discriminate against a consumer for exercising the rights provided to a consumer under this chapter.

(B) A business may charge different prices or rates for goods or services for individuals who exercise their rights under this chapter for legitimate business reasons or as otherwise permitted or required by applicable law.

(C) A business's denial of a consumer's request in compliance with this chapter shall not be considered discrimination against the consumer.

(D) Nothing in this section shall be construed as doing either of the following:

(1) Requiring a business to provide a product or service
that requires the personal data of a consumer that the business does not collect or maintain;

(2) Prohibiting a business from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised the right to opt-out pursuant to section 1355.06 of the Revised Code and if the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

Sec. 1355.08. (A) A business shall enter into a written contract with a processor that prohibits the processor from processing personal data except to provide services to the business.

(B) A business may allow the processor to do all of the following:

(1) Retain and employ a sub-processor, where the sub-processor meets the requirements for a processor under this chapter;

(2) Internal processing to improve the quality of its products or services, provided that the processing of personal data is in compliance with the requirements of this chapter;

(3) Detect or prevent data security incidents, fraud, or illegal activity;

(4) Use data as otherwise permitted by this chapter.

Sec. 1355.09. (A) The attorney general has exclusive authority to enforce this chapter.

(B) Except as provided in divisions (B)(1) to (4) of this section, if, by the attorney general's own inquiries or as a
result of complaints, the attorney general has reasonable cause to believe that a business has engaged or is engaging in an act or practice that violates this chapter, the attorney general may investigate in accordance with section 1345.06 of the Revised Code:

(1) References to "person" in section 1345.06 of the Revised Code shall be interpreted, for purposes of investigations entered into under this section, as referring to an individual or a business, as defined in section 1355.01 of the Revised Code.

(2) References to a "supplier" in section 1345.06 of the Revised Code shall be interpreted, for purposes of investigations entered into under this section, as referring to a business, as defined in section 1355.01 of the Revised Code.

(3) Division (E) of section 1345.06 of the Revised Code does not apply to investigations entered into under this section.

(4) Nothing in this section shall be construed as granting any additional rights or responsibilities under any other section of Chapter 1345 of the Revised Code.

(C) The attorney general shall not disclose publicly the identity of a business investigated under this section or the facts developed in investigations unless either of the following are met:

(1) These matters have become a matter of public record in enforcement proceedings, including if the business has entered into an assurance of voluntary compliance with the attorney general pursuant to section 1345.06 of the Revised Code.

(2) The business that is the subject of the investigation
has consented in writing to public disclosure.

(D)(1) If the attorney general, by the attorney general's own inquiries or as a result of complaints, has reasonable cause to believe that a business has engaged or is engaging in an act or practice that violates this chapter, the attorney general, subject to divisions (D)(2) to (4) of this section, may bring an action in a court of common pleas of this state seeking any or all of the following relief:

(a) Declaratory judgment that the act or practice violates this chapter;

(b) Injunctive relief, including preliminary and permanent injunctions, to prevent further violations of and compel compliance with this chapter;

(c) Civil penalties described in division (D)(2)(c) of this section;

(d) Attorneys' fees and investigative costs;

(e) Any other relief the court determines appropriate, including relief described in division (D)(4) of this section.

(2)(a) Prior to initiating any action under this section, the attorney general shall provide a business thirty-days' notice, in writing, identifying the specific provisions of this chapter the attorney general alleges have been or are being violated.

(b) If, within the thirty-day period, the business cures the noticed violation and provides the attorney general an express written statement that the alleged violations have been cured and that no further violations will occur, the attorney general shall not initiate an action against the business.
except as provided in division (D)(2)(c) of this section.

(c) If a business continues to violate this chapter following the cure period described in division (D)(2)(b) of this section or breaches an express written statement provided to the attorney general pursuant to that division, the attorney general may initiate an action pursuant to division (D)(1) of this section and seek civil penalties of up to five thousand dollars for each violation under this chapter.

(3) Civil penalties levied in accordance with this division shall be made in accordance with the following criteria:

(a) Each provision of this chapter that was violated counts as a separate violation.

(b) Each consumer affected counts as a separate violation.

(c) When calculating civil penalties, the court may consider all of the following:

(i) The number of affected consumers;

(ii) The severity of the violation;

(iii) The size, nature, and complexity of the business;

(iv) The sensitivity of the information in question;

(v) The precautions taken to prevent a violation.

(4)(a) Appropriate relief may be awarded to each identified consumer affected by a violation of a section of this chapter, regardless of whether any actual damages were suffered, in an amount that is not less than one hundred dollars and not more than seven hundred fifty dollars per violation.

(b) If the court finds the business willfully or knowingly
violated this chapter, the court may, in its discretion, triple the award.

(E) Any moneys awarded under this section, with the exception of amounts awarded under division (D)(4) of this section, shall be deposited into the consumer protection enforcement fund established in section 1345.51 of the Revised Code.

(F) The remedies available to the attorney general under this section are cumulative and concurrent, and the exercise of one remedy by the attorney general does not preclude or require the exercise of any other remedy.

(G) Any violation of this chapter shall not serve as the basis for, or be subject to, a private right of action, including a class action lawsuit, under this chapter or under any other law.

(H)(1) A business that discloses personal data to a processor shall not be liable under this chapter if the processor uses it in violation of the restrictions set forth in this chapter, provided that, at the time of disclosing the personal data, the business does not have actual knowledge, or reason to believe, that the processor intends to commit such a violation.

(2) A processor shall likewise not be liable under this chapter for the obligations of a business for which the processor provides services as set forth in this chapter.

(I)(1)(a) A business has an affirmative defense against allegations of violations of this chapter if that business creates, maintains, and complies with a written privacy program that reasonably conforms to the national institute of standards
and technology privacy framework entitled "A Tool for Improving Privacy through Enterprise Risk Management Version 1.0," including applicable controls selected by the business from special publication 800-53 and 800-53a published by the national institute of standards and technology and referenced by the national institute of standards and technology privacy framework.

(b) When a final revision to the national institute of standards and technology privacy framework is published, a business shall reasonably conform its privacy program to the revised framework not later than one year after the publication date stated in the revision.

(2) A business's privacy program shall be designed to provide individuals with the substantive rights provided to individuals by this chapter.

(3) The scale and scope of a business's privacy program under divisions (I)(1) and (2) of this section is appropriate if it is based on all of the following factors:

(a) The size and complexity of the business;
(b) The nature and scope of the activities of the business;
(c) The sensitivity of the personal information processed;
(d) The cost and availability of tools to improve privacy protections and data governance;
(e) Compliance with any comparable state or federal law.

(4) A business that satisfies divisions (I)(1), (2), and (3) of this section has an affirmative defense to any cause of action brought under the laws of this state or in the courts of
this state that alleges a violation of this chapter or similar claim based on a violation of privacy rights afforded to individuals under this chapter or under Chapter 1345. of the Revised Code, commonly referred to as the consumer sales practices act.

Section 2. The Attorney General may use $250,000 of appropriation item 055321, Operating Expenses, in fiscal year 2022 and fiscal year 2023 for the purpose of enforcing the Ohio Personal Privacy Act and enacted sections 1355.01 to 1355.09 of the Revised Code.