OHIO LEGISLATIVE SERVICE COMMISSION

www.lsc.ohio.gov

Office of Research and Drafting

Legislative Budget Office

H.B. 376*
134th General Assembly

# Bill Analysis

Click here for H.B. 376's Fiscal Note

**Version:** As Reported by House Government Oversight

**Primary Sponsors:** Reps. Carfagna and Hall

Nick Thomas, Research Analyst

## SUMMARY

- Provides consumers with the following rights:
  - A right to know what personal data a covered business collects about that consumer;
  - A right to access and receive personal data that a company has with regard to that consumer;
  - A right to request that incorrect personal data be corrected;
  - A right to request that personal data pertaining to that consumer be deleted;
  - A right to request that personal data pertaining to that consumer not be sold.
- Requires covered businesses to establish, maintain, and make available a privacy policy that describes how the business collects, uses, and sells consumer personal data.
- Requires covered businesses to comply with verified requests made in relation to the consumer rights provided by the bill and specifies deadlines for compliance.
- Establishes the Attorney General as the sole entity authorized to enforce the requirements of the bill via investigations and lawsuits, provides covered businesses a path for asserting an affirmative defense against such lawsuits, and specifies that the bill does not authorize consumers to bring lawsuits against covered businesses.
- Authorizes the Attorney General to use $250,000 of the Operating Expenses line item, in FY 2023, for the purpose of enforcing the bill's requirements.

* This analysis was prepared before the report of the House Government Oversight appeared in the House Journal. Note that the legislative history may be incomplete.

# TABLE OF CONTENTS

# DETAILED ANALYSIS

## Overview

The bill establishes requirements related to the collection, processing, and sale of digital personal data that will take effect one year after the bill's effective date. These requirements fall into two primary categories: requirements imposed on companies that collect or process personal data and rights provided to consumers whose personal data is collected. As used in the bill, "personal data" is any information that relates to an identified or identifiable consumer processed by a business for a commercial purpose. Personal data does not include publicly available information, deidentified, or aggregate information.[1]

## Application

The bill applies to a business that conducts business in Ohio, or whose products or services target consumers in Ohio, and that meets any of the following criteria:

- Gross annual revenue exceeds $25 million;
- Controls or processes personal data of 100,000 or more consumers during a calendar year;
- During a calendar year, derives more than 50% of gross revenue from (1) the sale of personal data and (2) processes or controls personal data of 25,000 or more consumers.[2]

## Consumer rights

The bill provides five basic rights to consumers with regard to their personal data: a right to know what data is collected about them, a right to request that data, a right to have their data deleted, a right to have their data corrected, and a right to prohibit the sale of their personal data. The bill imposes corresponding requirements on affected businesses.

## Consumer's right to know what data is collected

The bill provides consumers with a right to know what personal data a company collects about them.[3] The primary way that this requirement is met is through the company's privacy policy.

### Privacy policy

Businesses are required to provide consumers with information on the personal data it processes by providing a reasonably accessible, clear, and conspicuously posted privacy policy. The privacy policy must include all of the following:

[1] R.C. 1355.01(J) and Section 4.

[2] R.C. 1355.02(A).

[3] R.C. 1355.03(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;
- The categories of personal data the business processes;
- The purposes of processing each category of personal data;
- The categories of sources from which the personal data is collected;
- The categories of processors with whom the business discloses personal data;
- Whether or not the business sells personal data to third parties and, if the business makes such sales, the categories of third parties to whom the business sells personal data, and how a consumer may exercise the right to opt out of such processing;
- A description of the business's data retention practices for personal data and the purposes for such retention;
- How individuals can exercise their personal data rights;
- The effective date of the privacy policy;
- A description of the mechanism or mechanisms a business can use to notify consumers when it makes a material change to its privacy policy or decides to process personal data for purposes incompatible with the privacy policy.

The privacy policy must also disclose any and all commercial purposes for which the company collects or processes personal data. However, the bill specifies that it is not to be construed as authorizing a consumer to sue for a failure to comply with privacy policy requirement. 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 is to be considered an unfair and deceptive practice under the Consumer Sales Practices Act. And finally, a business, a co-business, or a processor may provide the privacy policy to the consumer on behalf of a primary business.[4]

## Material changes to privacy policy

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 must do either of the following prior to further processing previously collected personal data:

- Obtain affirmative consent from the consumers affected;
- 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.

[4] R.C. 1355.03(A), (B), (C), and (D).

A business is required to 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. If a company complies with this requirement via notice, the notice must be provided not less than 60 days prior to implementing the change, taking into account available technology and the nature of the relationship between the business and the consumer.[5]

# Consumer rights in relation to the data collected

The bill prescribes several rights for consumers with regard to their personal data. It also prescribes a uniform method of exercising those rights.

## Methods for exercising rights

The bill allows a consumer, or the parent or guardian of a known child (a person under 13) on the child's behalf, to exercise the rights provided under the bill by making a verifiable request. A business is required to provide at least one of the following methods for making such a request:

- A toll-free telephone number;
- An email address;
- A web form;
- A clear and conspicuous link on the business's main internet homepage to an internet webpage.

For consumers that maintain an account with the business in question, the business may require the consumer to submit the request through that account. However, if the consumer does not maintain an account with the business in question, the business is prohibited from requiring an account be made.

Prior to granting requests made in relation to personal data, businesses must first verify the requester's identity. If the business is not able to verify the consumer's identity, then the business is not required to comply with the request.

For verified requests, the business must comply with the request within 45 calendar days. For reasonable cause, and upon notice to the consumer, the business may take an additional 45 days to respond to the request. But such a delay may not be used more than once. Upon receipt of a verified request, a business must comply with all requirements associated with the rights provided by the bill, as described below, including notifying processors.[6]

[5] R.C. 1355.03(E) and (F).

[6] R.C. 1355.04 and 1355.01(D).

## Right to access the personal data collected

Under the bill, a consumer has a right to request may request a copy of the consumer's personal data that the consumer previously provided to the business electronically in a portable, and to the extent technically feasible, readily usable format.[7] After receiving a verified request, covered businesses must disclose both of the following for the preceding 12-month period:

- The categories of third parties to whom the business sells personal data, or if it does not sell personal data, that fact;
- The personal data the business has collected about the consumer.[8]

A business is not obligated to provide access to a consumer's personal data more than once in a 12-month period, beginning from the prior date on which the consumer made a request. Finally, a business may redact personal data in its responses to consumers to protect the security of personal data, including redacting Social Security numbers, financial account numbers, or driver's license numbers.[9]

## Right to correct personal data

Under the bill, a consumer has a right to correct inaccuracies in the consumer's personal data that the consumer previously provided to the business, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data, by making a verifiable request to have the consumer's data be corrected. Upon receiving a verified request, a business is required to correct inaccurate information as requested by the consumer, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data.[10]

## Right to delete the personal data collected

The bill provides consumers with 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. As with the right to access, this is done by a verifiable request. Such a request must reasonably describe the personal data the consumer is requesting deleted.[11]

If the consumer's personal data is stored on archived or backup systems, a covered business may delay compliance with a 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

[7] R.C. 1355.05(A).

[8] R.C. 1355.05(B) and (C).

[9] R.C. 1355.05(C) and (D).

[10] R.C. 1355.06.

[11] R.C. 1355.07(A) and (B).

sale, disclosure, or commercial purpose. 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.[12]

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. Also, a business, or an associated processor, is not to 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 adhere to its written records retention schedule.[13]

## Right to request personal data not be sold

The bill provides consumers with the right to request both of the following from a covered business:

- That the business not sell the consumer's data;
- That the business not process the consumer's personal data for the purposes of targeted advertising (advertising that uses personal data derived from a consumer's online activities to predict the consumer's preferences or interests).[14]

Upon receipt of a verified request, a business is prohibited from selling the personal data of the consumer in question or processing the data for targeted advertising. However, a business is not required to comply with an opt-out request that the business reasonably determines to be fraudulent. Once a request has been verified, businesses are also required, within reason, to inform their processors or third parties of a consumer's request to opt out and request that they also comply with the consumer's opt-out request.[15]

## Miscellaneous provisions relating to selling personal data

Even without a request, businesses are prohibited from selling the personal data that is collected online of children under 13 without complying with the "Children's Online Privacy Protection Act of 1998" and its regulations. Also, a business that sells personal data, or uses the processed data for the purposes of targeted advertising, is required to 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, the use of that data for targeted advertising, or both. Such a

[12] R.C. 1355.07(C) and (D).

[13] R.C. 1355.07(D) and (E).

[14] R.C. 1355.08(A) and 1355.01(P).

[15] R.C. 1355.08(B), (E), and (F).

notice can be made by providing clear and conspicuous notice on its website privacy policy or other publicly available notice.[16]

## Retaliation prohibited

Businesses are expressly prohibited from discriminating against a consumer for exercising the rights provided in the bill. However, the bill does authorize businesses to charge different prices or rates for goods or services for individuals who exercise their rights under the bill for legitimate business reasons or as otherwise permitted or required by applicable law. Note that a denial of a request related to personal data by a business is not considered discrimination. Also, the bill specifies that it is not to be construed as doing any of the following:

- 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;
- Requiring a business to provide a product or service if the consumer has requested that the consumer's data not be sold;
- 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 offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.[17]

## Relationship between data processors and covered businesses

The bill regulates the relationship between covered businesses and data processors in relation to personal data. A contract between a covered business and processor is required to govern the data processing procedures of the processor with respect to processing performed on behalf of the business. A processor must do all of the following:

- Taking into account the nature of the processing, assist a business, to the extent reasonably possible and through the use of appropriate technical and organizational measures, in fulfilling the obligation of the business to respond to consumer requests to exercise the rights provided in the bill;
- Develop, implement, and maintain reasonable administrative, technical, and physical safeguards to protect the security and confidentiality of personal data processed by the processor. The safeguards must reflect the nature and scope of the activities of the processor and its role in processing the personal data;
- At the direction of the business and pursuant to the contract described above, delete or return, except as required by law, all personal data to the business as requested at the end of the contract period;

[16] R.C. 1355.08(C) and (D) and 1355.01(D).

[17] R.C. 1355.09.

- If the processor uses the services of a subprocessor with respect to a business, require the subprocessor to meet the obligations of the processor with respect to any personal data collected.

At times, whether a person constitutes a business or a processor may be unclear. Under the bill, whether a person acts as a business or a processor with respect to a specific processing of personal data is a fact-based determination that depends on the context in which the personal data is processed. A processor adhering to the instructions of a business with respect to a specific processing of personal data is considered a processor. A processor, to the extent that it is acting in the role of a processor, is considered a processor and not a business.[18]

# Enforcement

The Attorney General is provided with exclusive authority to enforce the requirements of the bill. Furthermore, the bill expressly states that it is not to be construed as authorizing a consumer to bring a lawsuit for violations of the bill's requirements, including a class action lawsuit.[19]

## Investigations

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 or processor has engaged or is engaging in an act or practice that violates the bill's requirements, the Attorney General may investigate. Such an investigation is to be made in accordance with the law governing investigations of violations of the Consumer Sales Practices Act (CSPA), but with a few provisos. First, references to "person" in the CSPA are to be interpreted as referring to an individual or a business, as defined by the bill. Second, references to a "supplier" are to be interpreted as referring to a business as defined by the bill. Third, the bill specifies that a provision in the CSPA that allows the Attorney General to request a court to compel a person to testify does not apply with regard to personal data investigations. Finally, the bill specifies that it is not to be construed as granting any additional rights or responsibilities under the CSPA.[20]

## Disclosures

The Attorney General is prohibited from publicly disclosing the identity of a business or processor being investigated or the facts developed in investigations unless either of the following are met:

- 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 the CSPA;

[18] R.C. 1355.10 and 1355.01(C).

[19] R.C. 1355.11(A) and (G).

[20] R.C. 1355.11(B).

- The business or processor that is the subject of the investigation has consented in writing to public disclosure.[21]

## Enforcement via lawsuit

If the Attorney General has reasonable cause to believe that a covered business or processor has engaged or is engaging in an act or practice that violates the bill's requirements, the Attorney General may bring a lawsuit seeking any or all of the following forms of relief:

- Declaratory judgment that the act or practice violates the bill;
- Injunctive relief, including preliminary and permanent injunctions, to prevent further violations of and compel compliance with the bill;
- Civil penalties;
- Attorneys' fees and investigative costs;
- Any other relief the court determines appropriate, including relief provided to consumers affected by a violation.

Prior to initiating any such a lawsuit, the Attorney General is required to provide a 30-days' notice, in writing, identifying the specific provisions of the bill the Attorney General alleges have been or are being violated. If, within the 30-day period, the business or processor 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 is prohibited from initiating an action against the business or processor. However, if a business or processor continues to violate a representation made in such a written statement following the cure period or breaches an express written statement provided to the Attorney General, the Attorney General may initiate a lawsuit and seek civil penalties of up to $5,000 for each violation.[22]

### Civil penalties

Civil penalties are to be made in accordance with the following criteria:

- Each provision of the bill that was violated counts as a separate violation.
- Each consumer affected counts as a separate violation.
- When calculating civil penalties, the court may consider all of the following:
  - The number of affected consumers;
  - The severity of the violation;
  - The size, nature, and complexity of the business or processor;

[21] R.C. 1355.11(C).

[22] R.C. 1355.11(D)(1) and (2).

- The sensitivity of the information in question;
- The precautions taken to prevent a violation.

Appropriate relief may be awarded to each identified consumer affected by a violation of the bill's requirements, regardless of whether any actual damages were suffered, in an amount that is not less than $100 and not more than $750 per violation. If the court finds that the violation was willful or made knowingly, the court may triple the award.

Where more than one business or processor, or both a business and a processor, involved in the same processing violate the requirements of the bill, liability must be apportioned according to the amount of responsibility born by each.

Any moneys awarded, with the exception of amounts awarded directly to consumers, are to be deposited into the Consumer Protection Enforcement Fund. The bill specifies that the remedies available to the Attorney General 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.[23]

## Data processor liability

A business or processor that discloses personal data to another business or processor is not to be considered liable if the recipient uses the data in violation of the restrictions set forth by the bill, provided that, at the time of disclosing the personal data, the business or processor does not have actual knowledge, or reason to believe, that the processor intends to commit such a violation.[24]

## Affirmative defense

The bill provides an affirmative defense against lawsuits brought under the bill. However, in order to assert the defense, the covered business must satisfy all components of a three-prong test. First, the covered business must establish a privacy program that meets a national standard and provides individuals with the substantive rights provided under the bill. Second, that program must be kept up-to-date, mirroring the national standard. And third, the covered business's privacy program must be appropriate given the business's size and nature. These requirements are discussed in greater detail below.[25]

The first step to asserting an affirmative defense is the creation, maintenance, and compliance with a written privacy program that reasonably conforms to the National Institute of Standards and Technology (NIST) 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 NIST and referenced by the NIST privacy framework. When a final revision to the NIST privacy framework is published, a

[23] R.C. 1355.11(D)(3), (D)(4), (E), (F), and (J) and R.C. 1345.51.

[24] R.C. 1355.11(H).

[25] R.C. 1355.11(I)(3).

business is required to reasonably conform its privacy program to the revised framework not later than one year after the publication date stated in the revision.

The scale and scope of a business's privacy program is to be considered appropriate if all of the following factors have been taken into account:

- The size and complexity of the business;
- The nature and scope of the activities of the business;
- The sensitivity of the personal information processed;
- The cost and availability of tools to improve privacy protections and data governance;
- Compliance with any comparable state or federal law.[26]

## Exemptions

The bill's requirements do not apply to any of the following:

- Any body, authority, board, bureau, commission, district, or agency of the state or of any Ohio political subdivision;
- A financial institution, data, or an affiliate of a financial institution governed by Title V of the federal "Gramm-Leach-Bliley Act" and related regulations;
- A covered entity or business associate governed by the privacy, security, and breach notification rules issued by the U.S. Department of Health and Human Services and the Health Information Technology for Economic and Clinical Health Act;
- An institution of higher education;
- Business to business transactions;
- Any insurer or independent insurance agent;
- Any nonprofit organization established to detect or prevent insurance-related crime or fraud;
- Any insurer rates and filings advisory organization;
- Any Ohio-licensed insurance rating organization;
- Personal data regulated by the federal "Children's Online Privacy Protection Act," if collected, processed, and maintained in compliance with that law and its implementing regulations or exemptions.[27]

[26] R.C. 1355.11(I).

[27] R.C. 1355.02(B).

## Exempt data

The following information and data are also exempt from the bill's requirements:

- Protected health information under the Health Insurance Portability and Accountability Act (HIPAA);
- Health records;
- Patient identifying information, as defined under federal public health and welfare confidentiality requirements;
- Identifiable private information for purposes of the federal policy for the protection of human research subjects;
- 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 harmonization of technical requirements for pharmaceuticals for human use;
- Data related to the protection of human research subjects or personal data used or shared in research conducted in accordance with the requirements set forth in the bill, or other research conducted in accordance with applicable law;
- Information and documents created for purposes of the federal "Health Care Quality Improvement Act of 1986";
- Patient safety work product for purposes of the federal "Patient Safety and Quality Improvement Act";
- Information derived from any health care-related data that is deidentified in accordance with the requirements for deidentification pursuant to HIPAA;
- Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as exempt health and research information that is maintained by a covered entity or business associate, as defined by HIPAA or a program or a qualified service organization;
- Information used only for public health activities and purposes as authorized by HIPAA;
- 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";
- Personal data collected, processed, sold, or disclosed in compliance with the federal "Driver's Privacy Protection Act of 1994";
- Personal data regulated by the federal "Family Educational Rights and Privacy Act";

- Personal data collected, processed, sold, or disclosed in compliance with the federal "Farm Credit Act";
- Data processed or maintained in accordance with any of the following:
  - In the course of an individual applying to, employed by, or acting as an agent or independent contractor of a business subject to the bill, processor, or a related third party, to the extent that the data is collected and used within the context of that role;
  - For emergency contact purposes for individuals described above;
  - As necessary to administer employment benefits to those individuals above, as well as to any persons related to those individuals, such as dependents or spouses.[28]

## Exempt with regard to compliance

The bill's requirements do not apply to the extent necessary for a business or processor to do any of the following:

- Comply with federal or state law;
- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities;
- Cooperate with law enforcement agencies concerning conduct or activity that the business, processor, or third party reasonably and in good faith believes may violate federal, state, or local law;
- Exercise, or defend against, legal claims;
- Prevent, detect, or protect against, or provide a response to, security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity;
- Report or prosecute those responsible for any such action;
- Preserve the integrity or security of systems;
- 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;
- Assist another business, processor, or third party with any of the above obligations;
- Provide a product or service specifically requested by a consumer or a child's parent or guardian;

[28] R.C. 1355.02(C).

- Perform a contract to which a consumer or child's parent or guardian is a party, including fulfilling the terms of a written warranty;
- Comply with the request of a consumer or child's parent or guardian prior to entering into a contract;
- 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.[29]

## Interpretation and application

The bill specifies that its requirements do not apply to the extent that compliance with those requirements would violate or hinder an evidentiary privilege under Ohio law.

Furthermore, the bill is not to be construed as doing any of the following:

- Restricting a business's ability to collect, use, or retain data as necessary to do any of the following:
  - Conduct internal research solely to improve or repair products, services, or technology;
  - Identify and repair technical errors that impair existing or intended functionality;
  - 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;
  - Effectuate a product recall.
- Requiring a business or processor 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;
- 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;
- Applying to the processing of personal data by a natural person in the course of a purely personal or household activity.[30]

[29] R.C. 1355.02(D).

[30] R.C. 1355.02(E), (F), (G), and (H).

### Pseudonymous data

The bill specifies that the consumer rights provided in the Ohio Personal Privacy Act do not apply to pseudonymous data in cases where the business or processor is able to demonstrate that any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls to prevent the business or processor from accessing such information.[31]

### Trade secrets

The bill specifies that nothing in the Ohio Personal Privacy Act is to be construed as requiring a business or processor to disclose a trade secret.[32]

## Statewide, comprehensive enactment

The bill states that it is the intent of the General Assembly to establish a statewide, comprehensive enactment that applies to all parts of the state, operates uniformly throughout the state, and sets forth police regulations. No political subdivision is to regulate the collection, processing, or sale of personal data by a business.[33]

## Earmark

The bill authorizes the Attorney General to use $250,000 of the Operating Expenses line item, in FY 2023, for the purpose of enforcing the bill's requirements.[34]

## Definitions

The bill defines the following terms.

"**Affiliate**" means a legal entity that controls, is controlled by, shares common branding with, or is under common control with, another legal entity. For purposes of this definition, "control" or "controlled" means a relationship between two legal entities characterized by any of the following:

- One entity having ownership of, or the power to vote, more than 50% of the outstanding shares of any class of voting security of the other legal entity;
- 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;
- One entity having the power to exercise a controlling influence over the management of the other entity.

[31] R.C. 1355.02(I).

[32] R.C. 1355.02(J).

[33] R.C. 1355.11(K).

[34] Section 3.

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

"**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 Ohio, any other state, the United States, or any other country, that, alone or jointly with others, determines the purpose and means of processing personal data. "Business" does not include a public entity or a processor, to the extent that the processor is acting in the role of a processor.

"**Child**" means any natural person under 13.

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

- The person that is the subject of such information;
- Any third party.

"**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.

"**Consumer**" means a natural person who is an Ohio resident 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.

"**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.

"**HIPAA**" means the Health Insurance Portability and Accountability Act of 1996.

"**Personal data**" means any information that is linked or is reasonably linkable to an identified or identifiable consumer and that is processed by a business for a commercial purpose. "Personal data" does not include either of the following:

- Any such data processed from publicly available sources;
- Pseudonymized, deidentified, or aggregate data.

"**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.

"**Processor**" means a natural or legal person who processes personal data on behalf of a business subject to the bill.

"**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.

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

"**Sale**," "**sell**," or "**sold**" means the exchange of personal data for monetary or other valuable consideration by a business to a third party. "Sale," "sell," or "sold" does not include any of the following:

- The disclosure of personal data to a processor who processes the personal data on behalf of a business;
- The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer;
- The disclosure of personal data from one business to another business without monetary or other valuable consideration;
- The disclosure or transfer of personal data to an affiliate of the business;
- 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;
- 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.

"**Targeted advertising**" means displaying to a consumer an advertisement that is selected based on personal data obtained or inferred over time from the consumer's activities across nonaffiliated websites, applications, or online services to predict consumer preferences or interests. "Targeted advertising" does not include any of the following:

- Advertising to a consumer in response to the consumer's request for information or feedback;
- Advertisements based on activities within a business's or processor's own websites or online applications;
- Advertisements based on the context of a consumer's current search query, visit to a website, or online application;
- Processing personal data solely for measuring or reporting advertising performance, reach, or frequency.

"**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.

"**Verified request**" means a request submitted to a business in relation to the consumer rights provided by the bill that has been verified by the business as being made by the consumer in question or by the consumer's representative. As used in this definition, "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.[35]

# HISTORY

| Action | Date |
|---|---|
| Introduced | 07-12-21 |
| Reported, H. Government Oversight | --- |

H0376-RH-134/ar

[35] R.C. 1355.01.