134th General Assembly

Regular Session   **H. B. No. 376**

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,	1
1355.04, 1355.05, 1355.06, 1355.07, 1355.08, and	2
1355.09 of the Revised Code to enact the Ohio	3
Personal Privacy Act.	4

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

Section 1. That sections 1355.01, 1355.02, 1355.03,	5
1355.04, 1355.05, 1355.06, 1355.07, 1355.08, and 1355.09 of the	6
Revised Code be enacted to read as follows:	7
Sec. 1355.01. As used in this chapter:	8
(A)(1) "Affiliate" means a legal entity that controls, is	9
controlled by, shares common branding with, or is under common	10
control with, another legal entity.	11
(2) For purposes of division (A)(1) of this section,	12
"control" or "controlled" means a relationship between two legal	13
entities characterized by any of the following:	14
(a) One entity having ownership of, or the power to vote,	15
more than fifty per cent of the outstanding shares of any class	16

of voting security of the other legal entity;   17

(b) One entity having control in any manner over the   18
election of a majority of the directors, or of individuals   19
exercising similar functions, of the other entity;   20

(c) One entity having the power to exercise a controlling   21
influence over the management of the other entity.   22

(B) "Aggregated data" means personal data that has been   23
aggregated using commercially reasonable methods such that a   24
consumer cannot be reasonably identified.   25

(C) "Business" means any limited liability company,   26
limited liability partnership, corporation, sole proprietorship,   27
association, or other group, however organized and regardless of   28
whether operating for profit or not for profit, including a   29
financial institution organized, chartered, or holding a license   30
authorizing operation under the laws of this state, any other   31
state, the United States, or any other country, or the parent or   32
subsidiary of any of the foregoing. "Business" does not include   33
a public entity, including a political subdivision of this   34
state, a city, township, or a county.   35

(D) "Child" means any natural person under thirteen years   36
of age.   37

(E) "Commercial purpose" means the processing of   38
information for the purpose of obtaining any form of   39
consideration from either of the following: 40

(1) The person that is the subject of such information;   41

(2) Any third party.   42

(F) "Consent" means a clear affirmative act signifying a   43
freely given, specific, informed, and unambiguous indication of   44

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

45
46
47
48

49
50
51
52
53

54
55
56
57

58
59

60
61
62
63

64
65

66

67
68
69
70
71

72

processes personal data on behalf of a business subject to this   73

chapter.   74

(M) "Pseudonymized or pseudonymous data" means information   75

that no longer allows the identification of an individual   76

without combining it with other information, provided that such   77

additional information is kept separately and is subject to   78

appropriate technical and organizational measures to ensure that   79

the personal data is not attributed to an identified or   80

identifiable consumer.   81

(N) "Publicly available information" means information   82

that is lawfully made available from federal, state, or local   83

government records. "Publicly available information" includes   84

widely available media.   85

(O)(1) "Sale," "sell," or "sold" means the exchange of   86

personal data for monetary or other valuable consideration by a   87

business to a third party.   88

(2) "Sale," "sell," or "sold" does not include any of the   89

following: 90

(a) The disclosure of personal data to a processor who   91

processes the personal data on behalf of a business;   92

(b) The disclosure of personal data to a third party for   93

purposes of providing a product or service requested by the   94

consumer;   95

(c) The disclosure of personal data from one business to   96

another business without monetary or other valuable   97

consideration;   98

(d) The disclosure or transfer of personal data to an   99

affiliate of the business;   100

(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; 101 102 103

(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. 104 105 106 107 108 109 110 111

(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. 112 113 114

(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. 115 116 117 118

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. 119 120 121 122

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: 123 124 125 126

(1) The business's annual gross revenues generated in this state exceed twenty-five million dollars; 127 128

(2) During a calendar year, the business controls or 129

processes personal data of one hundred thousand or more 130

consumers; 131

(3) During a calendar year, the business derives over 132

fifty per cent of its gross revenue from the sale of personal 133

data and processes or controls personal data of twenty-five 134

thousand or more consumers. 135

(B) This chapter does not apply to any of the following: 136

(1) Any body, authority, board, bureau, commission, 137

district, or agency of this state or of any political 138

subdivision of this state; 139

(2) A financial institution, data, or an affiliate of a 140

financial institution governed by Title V of the federal "Gramm- 141

Leach-Bliley Act," 15 U.S.C. 6801 et seq. and related 142

regulations; 143

(3) A covered entity or business associate governed by the 144

privacy, security, and breach notification rules issued by the 145

United States department of health and human services, 45 C.F.R. 146

Parts 160 and 164 established pursuant to HIPAA, and the health 147

information technology for economic and clinical health act, 42 148

U.S.C. 300jj et seq; 149

(4) An institution of higher education. 150

(5) Business to business transactions. 151

(6) Any of the following: 152

(a) Any insurer or independent insurance agent, as defined 153

in section 3905.49 of the Revised Code; 154

(b) Any nonprofit organization established to detect or 155

prevent insurance-related crime or fraud; 156

(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.

(5) Information and documents created for purposes of the federal "Health Care Quality Improvement Act of 1986," 42 U.S.C.

157	
158	
159	
160	
161	
162	
163	
164	
165	
166	
167	
168	
169	
170	
171	
172	
173	
174	
175	
176	
177	
178	
179	
180	
181	
182	
183	

11101 et seq.;   184

(6) Patient safety work product for purposes of the   185
federal "Patient Safety and Quality Improvement Act," 42 U.S.C.   186
299b-21 et seq.;   187

(7) Information derived from any of the health care-   188
related information listed in division (C) of this section that   189
is deidentified in accordance with the requirements for   190
deidentification pursuant to HIPAA;   191

(8) Information originating from, and intermingled to be   192
indistinguishable with, or information treated in the same   193
manner as information exempt under division (C) of this section   194
that is maintained by a covered entity or business associate as   195
defined by HIPAA or a program or a qualified service   196
organization as defined by 42 U.S.C. 290dd-2;   197

(9) Information used only for public health activities and   198
purposes as authorized by HIPAA;   199

(10) The collection, maintenance, disclosure, sale,   200
communication, or use of any personal information bearing on a   201
consumer's credit worthiness, credit standing, credit capacity,   202
character, general reputation, personal characteristics, or mode   203
of living by a consumer reporting agency or furnisher that   204
provides information for use in a consumer report, and by a user   205
of a consumer report, but only to the extent that such activity   206
is regulated by and authorized under the federal "Fair Credit   207
Reporting Act," 15 U.S.C. 1681 et seq.;   208

(11) Personal data collected, processed, sold, or   209
disclosed in compliance with the federal "Driver's Privacy   210
Protection Act of 1994," 18 U.S.C. 2721 et seq.;   211

(12) Personal data regulated by the federal "Family   212

Educational Rights and Privacy Act," 20 U.S.C. 1232g et seq.;   213

(13) Personal data collected, processed, sold, or   214
disclosed in compliance with the federal "Farm Credit Act," 12   215
U.S.C. 2001 et seq.;   216

(14) Data processed or maintained in accordance with any   217
of the following: 218

(a) In the course of an individual applying to, employed   219
by, or acting as an agent or independent contractor of a   220
business subject to this chapter, processor, or a related third   221
party, to the extent that the data is collected and used within   222
the context of that role;   223

(b) For emergency contact purposes for individuals   224
described in division (C)(14)(a) of this section;   225

(c) As necessary to administer employment benefits to   226
those individuals described in division (C)(14)(a) of this   227
section, as well as to any persons related to those individuals,   228
such as dependents or spouses.   229

(D) This chapter does not apply to the extent necessary   230
for a business to do any of the following: 231

(1) Comply with federal or state law;   232

(2) Comply with a civil, criminal, or regulatory inquiry,   233
investigation, subpoena, or summons by federal, state, or local   234
authorities;   235

(3) Cooperate with law enforcement agencies concerning   236
conduct or activity that the business, service provider, or   237
third party reasonably and in good faith believes may violate   238
federal, state, or local law;   239

(4) Exercise, or defend against, legal claims; 240

(5)(a) Prevent, detect, or protect against, or provide a 241
response to, security incidents, identity theft, fraud, 242
harassment, malicious or deceptive activities, or any illegal 243
activity; 244

(b) Report or prosecute those responsible for any such 245
action. 246

(6) Preserve the integrity or security of systems; 247

(7) Engage in public or peer-reviewed scientific, 248
historical, or statistical research in the public interest that 249
adheres to all other applicable ethics and privacy laws, if the 250
deletion of the information is likely to render impossible or 251
seriously impair the achievement of the research and the 252
consumer in question has provided consent; 253

(8) Assist another business, processor, or third party 254
with any of the obligations imposed under division (C) of this 255
section. 256

(E) The requirements of this chapter do not apply to the 257
extent that compliance would violate or hinder an evidentiary 258
privilege under Ohio law. 259

(F) The obligations imposed on businesses or processors 260
under this chapter shall not be construed as restricting a 261
business's or processor's ability to collect, use, or retain 262
data as necessary to do any of the following: 263

(1) Conduct internal research solely to improve or repair 264
products, services, or technology; 265

(2) Identify and repair technical errors that impair 266
existing or intended functionality; 267

(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

268
269
270
271
272
273
274

275

276
277
278
279
280
281
282

283
284
285

286
287
288
289

290
291
292

293
294
295

296

personal data that it processes about the consumer by providing   297
a reasonably accessible, clear, and conspicuously posted privacy   298
policy.   299

      (C)(1) The privacy policy shall include all of the   300
following: 301

      (a) The identity and the contact information of the   302
business, including the business's contact for privacy and data   303
security inquiries, and the identity of any affiliate to which   304
personal data may be transferred by the business;   305

      (b) The categories of personal data the business   306
processes;   307

      (c) The purposes of processing for each category of   308
personal data;   309

      (d) The purposes for collecting or selling personal data;   310

      (e) The categories of sources from which the personal data   311
is collected;   312

      (f) The categories of processors with whom the business   313
discloses personal data;   314

      (g) Whether the business sells personal data, the   315
categories of third parties to whom the business sells personal   316
data, and the purposes of the sale;   317

      (h) A description of the business's data retention   318
practices for personal data and the purposes for such retention;   319

      (i) How individuals can exercise their rights under this   320
chapter;   321

      (j) A general description of the business's data security   322
practices;   323

(k) The effective date of the privacy policy; 324

(l) A description of how the business will notify 325
consumers, pursuant to division (E) of this section, when it 326
makes a material change to its privacy policy or decides to 327
process personal data for purposes incompatible with the privacy 328
policy. 329

(2)(a) The privacy policy shall also disclose any and all 330
commercial purposes for which the company collects or processes 331
personal data. 332

(b) Failure on the part of a business to maintain a 333
privacy policy that reflects the business's data privacy 334
practices to a reasonable degree of accuracy shall be considered 335
an unfair and deceptive practice under Chapter 1345. of the 336
Revised Code, except that a consumer shall not be entitled to a 337
private cause of action under that chapter for a failure to 338
comply with division (C)(2)(a) of this section. 339

(D) A business, a co-business, or a processor may provide 340
the privacy policy to the consumer. 341

(E) If a business makes a material change to its privacy 342
policy or decides to process personal data for purposes 343
incompatible with the privacy policy, it shall do either of the 344
following prior to further processing previously collected 345
personal data: 346

(1) Obtain affirmative consent from the consumers 347
affected; 348

(2)(a) Provide notice outlining the changes to the 349
business's privacy policy and providing affected consumers a 350
reasonable means to opt out of having their data processed or 351
disseminated. 352

(b) Such notice shall be provided not less than sixty days   353

prior to implementing the change, taking into account available   354

technology and the nature of the relationship between the   355

business and the consumer.   356

(F) The business shall provide direct notification, where   357

possible, regarding a material change to the privacy policy to   358

affected consumers, taking into account available technology and   359

the nature of the relationship.   360

Sec. 1355.04. (A) A consumer has a right to request access   361

to and the disclosure of the personal data that a business   362

collects about that consumer by making a verifiable request to   363

access the consumer's personal data.   364

(B)(1)(a) A business shall provide at least one of the   365

following methods for consumers to make requests under this   366

section: 367

(i) A toll-free telephone number;   368

(ii) An electronic mail address;   369

(iii) A web form;   370

(iv) A clear and conspicuous link on the business's main   371

internet homepage to an internet web page that enables a   372

consumer to exercise the rights provided under this section.   373

(b) However, if the consumer maintains an account with the   374

business, the business may require the consumer to submit the   375

request through that account. If the consumer does not maintain   376

an account, the business shall not require that an account be   377

created to submit the request.   378

(2) A business shall reasonably verify the identity of the   379

consumer before providing access and disclosing data under this   380

section.   381

(3) Upon receiving a verified request, a business shall   382
disclose both of the following to the consumer in question in   383
conformance with this section: 384

(a) The categories of third parties to whom the business   385
sells personal data, or if it does not sell personal data, that   386
fact;   387

(b) The personal data the business has collected about the   388
consumer.   389

(4) A business need not respond to a consumer request made   390
under this section if the business is unable to reasonably   391
verify the consumer.   392

(C) The disclosure shall cover the twelve-month period   393
preceding the business's receipt of the request.   394

(D)(1) A business shall provide the requested personal   395
data free of charge, within forty-five calendar days of the   396
request.   397

(2)(a) For reasonable cause, and upon notice to the   398
consumer citing the cause for the delay, a business may extend   399
the time required to respond to a request under this section by   400
an additional forty-five calendar days.   401

(b) Such a delay shall not be used more than one time.   402

(E) The consumer may request that the consumer's personal   403
data be provided electronically in a portable, readily usable   404
format or using paper mailed to the consumer.   405

(F) A business is not obligated to provide access to a   406
consumer's personal data more than once in a twelve-month   407

period, beginning from the prior date on which the consumer made 408
a request pursuant to this section. 409

(G) A business may redact personal data in its responses 410
to consumers to protect the security of personal data, 411
including, without limitation, redacting social security 412
numbers, financial account numbers, or driver's license numbers. 413

Sec. 1355.05. (A) A consumer shall have the right to 414
request that a business delete personal data that the business 415
has collected from the consumer for commercial purposes and that 416
the business maintains in an electronic format. 417

(B)(1)(a) A business shall provide at least one of the 418
following methods for consumers to make requests under this 419
section: 420

(i) A toll-free telephone number; 421

(ii) An electronic mail address; 422

(iii) A web form; 423

(iv) A clear and conspicuous link on the business's main 424
internet homepage to an internet web page that enables a 425
consumer to exercise the rights provided under this section. 426

(b) Consumers may submit a verifiable request to delete 427
personal data in writing to the business. However, if a consumer 428
maintains an account with the business, the business may require 429
the consumer to submit the request through that account. 430

(2) Such a verifiable request shall reasonably describe 431
the personal data the consumer is requesting be deleted. 432

(3) A business need not respond to a consumer request made 433
under this section if the business is unable to reasonably 434

verify the consumer. 435

(4) Within forty-five calendar days after verifying the 436
consumer's identity, a business shall either delete the personal 437
data or notify the consumer of its refusal to make such deletion 438
and the reason for refusal. 439

(C)(1) If the consumer's personal data is stored on 440
archived or backup systems, the business may delay compliance 441
with the consumer's request to delete until the archived or 442
backup system relating to that data is restored to an active 443
system, next accessed, or used for a sale, disclosure, or 444
commercial purpose. 445

(2) If the consumer's personal data is stored on archived 446
or backup systems, the business may comply with the consumer's 447
request by deleting or overwriting the data in accordance with a 448
scheduled backup or creation of a new archive, so long as the 449
business employs encryption standards to protect that data both 450
when the data is in transit and is at rest. 451

(D) A business is not required to delete personal data 452
that it maintains or uses as aggregated, deidentified, or 453
pseudonymous data, provided that such data in the possession of 454
the business is not linked to a specific consumer. 455

(E) A business, or an associated processor, shall not be 456
required to comply with a consumer's request to delete personal 457
data if it is necessary for the business or service provider to 458
maintain the consumer's personal data in order to do any of the 459
following: 460

(1) Comply with federal, state, or local laws, rules, or 461
regulations; 462

(2) Comply with a civil, criminal, or regulatory inquiry, 463

investigation, subpoena, or summons by federal, state, local, or 464
other governmental authorities; 465

(3) Adhere to its written records retention schedule; 466

(4) Cooperate with law enforcement agencies concerning 467
conduct or activity that the business, or service provider, 468
reasonably and in good faith believes may violate federal, 469
state, or local laws, rules, or regulations; 470

(5) Investigate, establish, exercise, prepare for, or 471
defend legal claims; 472

(6) Provide a product or service specifically requested by 473
a consumer, or reasonably anticipated within the context of the 474
business's ongoing business relationship with the consumer, or 475
otherwise perform a contract or warranty to which the consumer 476
is a party, or take steps at the request of the consumer prior 477
to entering into a contract; 478

(7) Take immediate steps to protect an interest that is 479
essential for the life of the consumer or of another natural 480
person, and where the processing cannot be manifestly based on 481
another legal basis; 482

(8) Prevent, detect, protect against, or respond to 483
security incidents, identity theft, fraud, harassment, malicious 484
or deceptive activities, or any illegal activity; 485

(9) Preserve the integrity or security of systems; 486

(10) Investigate, report, or prosecute those responsible 487
for any such action described in divisions (E)(8) and (9) of 488
this section; 489

(11) Engage, with the consent of the consumer, in public 490
or peer-reviewed scientific, historical, or statistical research 491

in the public interest that adheres to all other applicable   492

ethics and privacy laws if the deletion of the information is   493

likely to render impossible or seriously impair the achievement   494

of the research;   495

(12) Assist another party with any of the obligations   496

prescribed in division (E) of this section.   497

Sec. 1355.06. (A) A consumer has a right to request that a   498

business that sells personal data to third parties not sell the   499

consumer's personal data.   500

(B)(1) A business shall provide at least one of the   501

following methods for consumers to make a request under this   502

section: 503

(a) A toll-free telephone number;   504

(b) An electronic mail address;   505

(c) A web form;   506

(d) A clear and conspicuous link on the business's main   507

internet homepage to an internet web page that enables a   508

consumer to exercise the rights provided under this section.   509

(2) Upon receipt of a verified request made under division   510

(A) of this section, a business shall not sell the personal data   511

of the consumer in question.   512

(3) Verification shall be completed or, if appropriate   513

contact information can reasonably be obtained per the   514

consumer's request, the consumer shall be contacted to complete   515

verification without unreasonable delay, at most within thirty   516

calendar days.   517

(C) A business shall not sell the personal data of   518

children without complying with the "Children's Online Privacy 519
Protection Act of 1998," 15 U.S.C. 6501, et seq. 520

(D) A business that sells personal data shall provide 521
clear and conspicuous notice of this fact in such a manner as to 522
enable a consumer to opt out of the sale of the consumer's 523
personal data; such as by providing clear and conspicuous notice 524
on its web site privacy policy or other publicly available 525
notice. 526

(E) A business is not required to comply with an opt-out 527
request that the business reasonably determines to be 528
fraudulent. 529

(F) A business shall inform its processors or third 530
parties of a consumer's request to opt out and request that they 531
comply with the consumer's opt-out request. 532

Sec. 1355.07. (A) Subject to divisions (B) and (C) of this 533
section, a business shall not discriminate against a consumer 534
for exercising the rights provided to a consumer under this 535
chapter. 536

(B) A business may charge different prices or rates for 537
goods or services for individuals who exercise their rights 538
under this chapter for legitimate business reasons or as 539
otherwise permitted or required by applicable law. 540

(C) A business's denial of a consumer's request in 541
compliance with this chapter shall not be considered 542
discrimination against the consumer. 543

(D) Nothing in this section shall be construed as doing 544
either of the following: 545

(1) Requiring a business to provide a product or service 546

that requires the personal data of a consumer that the business   547
does not collect or maintain;   548

    (2) Prohibiting a business from offering a different   549
price, rate, level, quality, or selection of goods or services   550
to a consumer, including offering goods or services for no fee,   551
if the consumer has exercised the right to opt-out pursuant to   552
section 1355.06 of the Revised Code and if the offer is related   553
to a consumer's voluntary participation in a bona fide loyalty,   554
rewards, premium features, discounts, or club card program.   555

    Sec. 1355.08. (A) A business shall enter into a written   556
contract with a processor that prohibits the processor from   557
processing personal data except to provide services to the   558
business.   559

    (B) A business may allow the processor to do all of the   560
following: 561

    (1) Retain and employ a sub-processor, where the sub-   562
processor meets the requirements for a processor under this   563
chapter;   564

    (2) Internal processing to improve the quality of its   565
products or services, provided that the processing of personal   566
data is in compliance with the requirements of this chapter;   567

    (3) Detect or prevent data security incidents, fraud, or   568
illegal activity;   569

    (4) Use data as otherwise permitted by this chapter.   570

    Sec. 1355.09. (A) The attorney general has exclusive   571
authority to enforce this chapter.   572

    (B) Except as provided in divisions (B)(1) to (4) of this   573
section, if, by the attorney general's own inquiries or as a   574

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

575
576
577
578
579

580
581
582
583
584

585
586
587
588

589
590
591

592
593
594

595
596
597
598

599
600
601
602

603

has consented in writing to public disclosure. 604

(D)(1) If the attorney general, by the attorney general's 605
own inquiries or as a result of complaints, has reasonable cause 606
to believe that a business has engaged or is engaging in an act 607
or practice that violates this chapter, the attorney general, 608
subject to divisions (D)(2) to (4) of this section, may bring an 609
action in a court of common pleas of this state seeking any or 610
all of the following relief: 611

(a) Declaratory judgment that the act or practice violates 612
this chapter; 613

(b) Injunctive relief, including preliminary and permanent 614
injunctions, to prevent further violations of and compel 615
compliance with this chapter; 616

(c) Civil penalties described in division (D)(2)(c) of 617
this section; 618

(d) Attorneys' fees and investigative costs; 619

(e) Any other relief the court determines appropriate, 620
including relief described in division (D)(4) of this section. 621

(2)(a) Prior to initiating any action under this section, 622
the attorney general shall provide a business thirty-days' 623
notice, in writing, identifying the specific provisions of this 624
chapter the attorney general alleges have been or are being 625
violated. 626

(b) If, within the thirty-day period, the business cures 627
the noticed violation and provides the attorney general an 628
express written statement that the alleged violations have been 629
cured and that no further violations will occur, the attorney 630
general shall not initiate an action against the business, 631

except as provided in division (D)(2)(c) of this section. 632

(c) If a business continues to violate this chapter 633
following the cure period described in division (D)(2)(b) of 634
this section or breaches an express written statement provided 635
to the attorney general pursuant to that division, the attorney 636
general may initiate an action pursuant to division (D)(1) of 637
this section and seek civil penalties of up to five thousand 638
dollars for each violation under this chapter. 639

(3) Civil penalties levied in accordance with this 640
division shall be made in accordance with the following 641
criteria: 642

(a) Each provision of this chapter that was violated 643
counts as a separate violation. 644

(b) Each consumer affected counts as a separate violation. 645

(c) When calculating civil penalties, the court may 646
consider all of the following: 647

(i) The number of affected consumers; 648

(ii) The severity of the violation; 649

(iii) The size, nature, and complexity of the business; 650

(iv) The sensitivity of the information in question; 651

(v) The precautions taken to prevent a violation. 652

(4)(a) Appropriate relief may be awarded to each 653
identified consumer affected by a violation of a section of this 654
chapter, regardless of whether any actual damages were suffered, 655
in an amount that is not less than one hundred dollars and not 656
more than seven hundred fifty dollars per violation. 657

(b) If the court finds the business willfully or knowingly 658

violated this chapter, the court may, in its discretion, triple   659
the award.   660

    (E) Any moneys awarded under this section, with the   661
exception of amounts awarded under division (D)(4) of this   662
section, shall be deposited into the consumer protection   663
enforcement fund established in section 1345.51 of the Revised   664
Code.   665

    (F) The remedies available to the attorney general under   666
this section are cumulative and concurrent, and the exercise of   667
one remedy by the attorney general does not preclude or require   668
the exercise of any other remedy.   669

    (G) Any violation of this chapter shall not serve as the   670
basis for, or be subject to, a private right of action,   671
including a class action lawsuit, under this chapter or under   672
any other law.   673

    (H)(1) A business that discloses personal data to a   674
processor shall not be liable under this chapter if the   675
processor uses it in violation of the restrictions set forth in   676
this chapter, provided that, at the time of disclosing the   677
personal data, the business does not have actual knowledge, or   678
reason to believe, that the processor intends to commit such a   679
violation.   680

    (2) A processor shall likewise not be liable under this   681
chapter for the obligations of a business for which the   682
processor provides services as set forth in this chapter.   683

    (I)(1)(a) A business has an affirmative defense against   684
allegations of violations of this chapter if that business   685
creates, maintains, and complies with a written privacy program   686
that reasonably conforms to the national institute of standards   687

and technology privacy framework entitled "A Tool for Improving   688
Privacy through Enterprise Risk Management Version 1.0,"   689
including applicable controls selected by the business from   690
special publication 800-53 and 800-53a published by the national   691
institute of standards and technology and referenced by the   692
national institute of standards and technology privacy   693
framework.   694

     (b) When a final revision to the national institute of   695
standards and technology privacy framework is published, a   696
business shall reasonably conform its privacy program to the   697
revised framework not later than one year after the publication   698
date stated in the revision.   699

     (2) A business's privacy program shall be designed to   700
provide individuals with the substantive rights provided to   701
individuals by this chapter.   702

     (3) The scale and scope of a business's privacy program   703
under divisions (I)(1) and (2) of this section is appropriate if   704
it is based on all of the following factors: 705

     (a) The size and complexity of the business;   706

     (b) The nature and scope of the activities of the   707
business;   708

     (c) The sensitivity of the personal information processed;   709

     (d) The cost and availability of tools to improve privacy   710
protections and data governance;   711

     (e) Compliance with any comparable state or federal law.   712

     (4) A business that satisfies divisions (I)(1), (2), and   713
(3) of this section has an affirmative defense to any cause of   714
action brought under the laws of this state or in the courts of   715

this state that alleges a violation of this chapter or similar 716

claim based on a violation of privacy rights afforded to 717

individuals under this chapter or under Chapter 1345. of the 718

Revised Code, commonly referred to as the consumer sales 719

practices act. 720

Section 2. The Attorney General may use $250,000 of 721

appropriation item 055321, Operating Expenses, in fiscal year 722

2022 and fiscal year 2023 for the purpose of enforcing the Ohio 723

Personal Privacy Act and enacted sections 1355.01 to 1355.09 of 724

the Revised Code. 725