135th General Assembly

Regular Session   **H. B. No. 345**

2023-2024

Representatives Hall, Seitz

A BILL

To amend section 1345.51 and to enact sections	1
1357.01, 1357.02, 1357.03, 1357.04, 1357.05,	2
1357.06, 1357.07, 1357.08, 1357.09, 1357.10, and	3
1357.11 of the Revised Code to enact the Ohio	4
Personal Privacy Act.	5

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

Section 1. That section 1345.51 be amended and sections	6
1357.01, 1357.02, 1357.03, 1357.04, 1357.05, 1357.06, 1357.07,	7
1357.08, 1357.09, 1357.10, and 1357.11 of the Revised Code be	8
enacted to read as follows:	9
Sec. 1345.51. <u>(A)</u> There is hereby created in the state	10
treasury the consumer protection enforcement fund. The fund	11
shall include ~~civil~~ <u>all of the following:</u>	12
<u>(1) Civil</u> penalties ordered pursuant to divisions (A) and	13
(D) of section 1345.07 of the Revised Code and paid as provided	14
in division (G) of that section~~, all~~<u>;</u>	15
<u>(2) All</u> civil penalties assessed under division (A) of	16
section 1349.192 of the Revised Code~~, all~~<u>;</u>	17
<u>(3) All moneys awarded under section 1357.11 of the</u>	18

Revised Code other than amounts awarded pursuant to division (D) 19

(4) of that section; 20

(4) All costs awarded to the attorney general and all 21

penalties imposed under section 4549.48 of the Revised Code~~, and~~ 22

~~all~~; 23

(5) All money unclaimed under section 4549.50 of the 24

Revised Code. 25

(B) The money in the consumer protection enforcement fund 26

shall be used for the sole purpose of paying expenses incurred 27

by the consumer protection section of the office of the attorney 28

general. 29

Sec. 1357.01. As used in this chapter: 30

(A)(1) "Affiliate" means a legal entity that controls, is 31

controlled by, shares common branding with, or is under common 32

control with, another legal entity. 33

(2) For purposes of division (A)(1) of this section, 34

"control" or "controlled" means a relationship between two legal 35

entities characterized by any of the following: 36

(a) One entity having ownership of, or the power to vote, 37

more than fifty per cent of the outstanding shares of any class 38

of voting security of the other legal entity; 39

(b) One entity having control in any manner over the 40

election of a majority of the directors, or of individuals 41

exercising similar functions, of the other entity; 42

(c) One entity having the power to exercise a controlling 43

influence over the management of the other entity. 44

(B) "Aggregated data" means personal data that has been 45

aggregated using commercially reasonable methods such that a   46

consumer cannot be reasonably identified.   47

(C) "Business" means any limited liability company,   48

limited liability partnership, corporation, sole proprietorship,   49

association, or other group, however organized and regardless of   50

whether operating for profit or not for profit, including a   51

financial institution organized, chartered, or holding a license   52

authorizing operation under the laws of this state, any other   53

state, the United States, or any other country, that, alone or   54

jointly with others, determines the purpose and means of   55

processing personal data. "Business" does not include a public   56

entity, including this state, a political subdivision of this   57

state, or a processor to the extent that the processor is acting   58

in the role of a processor.   59

(D) "Child" means any natural person under thirteen years   60

of age.   61

(E) "Consent" means a clear affirmative act signifying a   62

freely given, specific, informed, and unambiguous indication of   63

a consumer's agreement to the processing of personal data   64

relating to the consumer, such as by a written statement,   65

including by electronic means, or other course of action that   66

would clearly indicate that consent has been provided.   67

(F) "Consumer" means a natural person who is a resident of   68

this state acting only in an individual or household context.   69

"Consumer" does not include a natural person acting in a   70

business capacity or employment context, including contractors,   71

job applicants, officers, directors, or owners.   72

(G) "Deidentified data" means personal data that has been   73

deidentified using commercially reasonable methods such that a   74

consumer, or a device linked to a consumer, cannot be reasonably identified. 75 76

(H) "HIPAA" has the same meaning as in section 3965.01 of the Revised Code. 77 78

(I) "Personal data" means any information that is linked or reasonably linkable to an identified or identifiable consumer and that is processed by a business. "Personal data" does not include either of the following: 79 80 81 82

(1) Any such data processed from publicly available sources; 83 84

(2) Deidentified or aggregate data. 85

(J) "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. 86 87 88 89 90

(K) "Processor" means a natural or legal person who processes personal data on behalf of a business subject to this chapter. 91 92 93

(L) "Pseudonymized or pseudonymous data" means data 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. 94 95 96 97 98 99 100

(M) "Publicly available information" means information that is lawfully made available from federal, state, or local 101 102

government records or widely available media. 103

(N)(1) "Sale," "sell," or "sold" means the exchange of 104
personal data for monetary or other valuable consideration by a 105
business to a third party. 106

(2) "Sale," "sell," or "sold" does not include any of the 107
following: 108

(a) The disclosure of personal data to a processor who 109
processes the personal data on behalf of a business; 110

(b) The disclosure of personal data to a third party for 111
purposes of providing a product or service requested by the 112
consumer; 113

(c) The disclosure of personal data from one business to 114
another business without monetary or other valuable 115
consideration; 116

(d) The disclosure or transfer of personal data to an 117
affiliate of the business; 118

(e) The disclosure of information that a consumer 119
intentionally made available to the general public via a channel 120
of mass media and did not restrict to a specific audience; 121

(f) The disclosure or transfer of personal data to a third 122
party as an asset that is part of a merger, acquisition, 123
bankruptcy, or other transaction in which the third party 124
assumes control of all or part of the business's assets. 125

(O) "Targeted advertising" means displaying to a consumer 126
an advertisement that is selected based on personal data 127
obtained or inferred over time from the consumer's activities 128
across nonaffiliated web sites, applications, or online services 129
to predict consumer preferences or interests. "Targeted 130

advertising" does not include any of the following: 131

(1) Advertising to a consumer in response to the   132
consumer's request for information or feedback;   133

(2) Advertisements based on activities within a business's   134
or processor's own web sites or online applications;   135

(3) Advertisements based on the context of a consumer's   136
current search query, visit to a web site, or online   137
application;   138

(4) Processing personal data solely for measuring or   139
reporting advertising performance, reach, or frequency.   140

(P) "Third party" means a natural or legal person, public   141
authority, agency, or body other than the consumer, business, or   142
processor, or an affiliate of the business or processor.   143

(Q) "Verified request" means a request submitted to a   144
business under sections 1357.03 to 1357.06 of the Revised Code   145
that has been verified by the business as being made by the   146
consumer in question or by the consumer's representative.   147

(R) "Consumer's representative" means a child's parent or   148
guardian or a representative of a person for whom a guardian of   149
the estate or conservator has been appointed.   150

   Sec. 1357.02. (A) This chapter applies to businesses that   151
conduct business in this state, or produce products or services   152
targeted to consumers in this state, that satisfy one or more of   153
the following criteria: 154

(1) The business's annual gross revenues generated in this   155
state exceed twenty-five million dollars;   156

(2) During a calendar year, the business controls or   157

processes personal data of one hundred thousand or more 158
consumers; 159

(3) During a calendar year, the business derives over 160
fifty per cent of its gross revenue from the sale of personal 161
data and processes or controls personal data of twenty-five 162
thousand or more consumers. 163

(B) This chapter does not apply to any of the following: 164

(1) Any body, authority, board, bureau, commission, 165
district, or agency of this state or of any political 166
subdivision of this state; 167

(2) A financial institution, data, or an affiliate of a 168
financial institution governed by Title V of the federal "Gramm- 169
Leach-Bliley Act," 15 U.S.C. 6801, et seq. and related 170
regulations; 171

(3) A covered entity or business associate governed by the 172
privacy, security, and breach notification rules issued by the 173
United States department of health and human services, 45 C.F.R. 174
160 and 164 established pursuant to HIPAA, and the federal 175
"Health Information Technology for Economic and Clinical Health 176
Act," 42 U.S.C. 300jj, et seq; 177

(4) An institution of higher education; 178

(5) Business to business transactions; 179

(6) Any of the following: 180

(a) Any insurer or independent insurance agent, as defined 181
in section 3905.49 of the Revised Code; 182

(b) Any nonprofit organization established to detect or 183
prevent insurance-related crime or fraud; 184

(c) Any advisory organization described in section 3937.09 of the Revised Code; 185
186

(d) Any rating organization licensed pursuant to section 3937.05 of the Revised Code or an affiliate thereof. 187
188

(7) Personal data regulated by the federal "Children's Online Privacy Protection Act," 15 U.S.C. 6501 to 6506, if collected, processed, and maintained in compliance with that law and its implementing regulations or exemptions. 189
190
191
192

(C) The following information and data are exempt from this chapter: 193
194

(1) Protected health information, as defined by 45 C.F.R. 160.103; 195
196

(2) Health records, as described in Chapter 3798. of the Revised Code; 197
198

(3) Patient identifying information for purposes of 42 U.S.C. 290dd-2; 199
200

(4) Any of the following types of information or data: 201

(a) Identifiable private information for purposes of the federal policy for the protection of human subjects under 45 C.F.R. 46; 202
203
204

(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; 205
206
207
208
209

(c) Data related to the protection of human subjects under 21 C.F.R. 6, 50, and 56, or personal data used or shared in 210
211

research conducted in accordance with the requirements set forth 212

in this chapter, or other research conducted in accordance with 213

applicable law. 214

(5) Information and documents created for purposes of the 215

federal "Health Care Quality Improvement Act of 1986," 42 U.S.C. 216

11101 et seq.; 217

(6) Patient safety work product for purposes of the 218

federal "Patient Safety and Quality Improvement Act," 42 U.S.C. 219

299b-21 et seq.; 220

(7) Information derived from any of the health care- 221

related information listed in division (C) of this section that 222

is deidentified in accordance with the requirements for 223

deidentification under HIPAA; 224

(8) Information originating from, and intermingled to be 225

indistinguishable with, or information treated in the same 226

manner as information exempt under division (C) of this section 227

that is maintained by a covered entity or business associate as 228

defined by HIPAA or a program or a qualified service 229

organization as defined by 42 U.S.C. 290dd-2; 230

(9) Information used only for public health activities and 231

purposes as authorized by HIPAA; 232

(10) The collection, maintenance, disclosure, sale, 233

communication, or use of any personal information bearing on a 234

consumer's credit worthiness, credit standing, credit capacity, 235

character, general reputation, personal characteristics, or mode 236

of living by a consumer reporting agency or furnisher that 237

provides information for use in a consumer report, and by a user 238

of a consumer report, but only to the extent that such activity 239

is regulated by and authorized under the federal "Fair Credit 240

Reporting Act," 15 U.S.C. 1681 et seq.;   241

(11) Personal data collected, processed, sold, or   242
disclosed in compliance with the federal "Driver's Privacy   243
Protection Act of 1994," 18 U.S.C. 2721 et seq.;   244

(12) Personal data regulated by the federal "Family   245
Educational Rights and Privacy Act," 20 U.S.C. 1232g et seq.;   246

(13) Personal data collected, processed, sold, or   247
disclosed in compliance with the federal "Farm Credit Act," 12   248
U.S.C. 2001 et seq.;   249

(14) Data processed or maintained in accordance with any   250
of the following: 251

(a) In the course of an individual applying to, employed   252
by, or acting as an agent or independent contractor of a   253
business subject to this chapter, processor, or a related third   254
party, to the extent that the data is collected and used within   255
the context of that role;   256

(b) For emergency contact purposes for individuals   257
described in division (C)(14)(a) of this section;   258

(c) As necessary to administer employment benefits to   259
those individuals described in division (C)(14)(a) of this   260
section, as well as to any persons related to those individuals,   261
such as dependents or spouses.   262

(D) This chapter does not apply to the extent necessary   263
for a business or processor to do any of the following: 264

(1) Comply with federal or state law;   265

(2) Comply with a civil, criminal, or regulatory inquiry,   266
investigation, subpoena, or summons by federal, state, or local   267

authorities; 268

(3) Cooperate with law enforcement agencies concerning 269
conduct or activity that the business, the processor, or a third 270
party reasonably and in good faith believes may violate federal, 271
state, or local law; 272

(4) Exercise, or defend against, legal claims; 273

(5)(a) Prevent, detect, or protect against, or provide a 274
response to, security incidents, identity theft, fraud, 275
harassment, malicious or deceptive activities, or any illegal 276
activity; 277

(b) Report or prosecute those responsible for any such 278
action. 279

(6) Preserve the integrity or security of systems; 280

(7) Engage in public or peer-reviewed scientific, 281
historical, or statistical research in the public interest that 282
adheres to all other applicable ethics and privacy laws, if the 283
deletion of the information is likely to render impossible or 284
seriously impair the achievement of the research and the 285
consumer in question has provided consent; 286

(8) Assist another business, processor, or third party 287
with any of the obligations imposed under division (C) of this 288
section; 289

(9) Provide a product or service specifically requested by 290
a consumer or a child's parent or guardian; 291

(10) Perform a contract to which a consumer or child's 292
parent or guardian is a party, including fulfilling the terms of 293
a written warranty; 294

(11) Comply with the request of a consumer or child's
parent or guardian prior to entering into a contract;

(12) 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.

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

(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 or processor to collect personal data that it would not
otherwise collect in the ordinary course of its business, retain

295
296

297
298
299
300

301
302
303

304
305
306
307

308
309

310
311

312
313
314
315
316
317
318

319

320
321
322

personal data for longer than it would otherwise retain such 323
data in the ordinary course of its business, or reidentify or 324
otherwise link information that is not maintained in a manner 325
that would be considered personal data. 326

(H) Obligations imposed on businesses and processors under 327
this chapter shall not be construed as doing either of the 328
following: 329

(1) Adversely affecting the rights or freedoms of any 330
persons, such as exercising the right of free speech pursuant to 331
the first amendment of the United States Constitution or Article 332
I, Section 11, of the Ohio Constitution; 333

(2) Applying to the processing of personal data by a 334
natural person in the course of a purely personal or household 335
activity. 336

(I) Nothing in this chapter shall be construed to do 337
either of the following: 338

(1) Require a business or processor to reidentify 339
deidentified data or pseudonymous data; 340

(2) Maintain data in an identifiable form or collect, 341
obtain, retain, or access any data or technology in order to be 342
capable of associating an authenticated consumer request with 343
personal data. 344

(J) The consumer rights provided under sections 1357.04 to 345
1357.08 of the Revised Code do not apply to pseudonymous data in 346
cases where the business or processor is able to demonstrate 347
that any information necessary to identify the consumer is kept 348
separately and is subject to effective technical and 349
organizational controls to prevent the business or processor 350
from accessing such information. 351

(K) Nothing in this chapter requires a business or   352
processor to disclose a trade secret.   353

    Sec. 1357.03. (A) A consumer has a right to know the   354
personal data that a business collects about that consumer, such   355
as by obtaining a privacy policy from the business.   356

    (B) A business shall provide consumers notice about the   357
personal data that it processes about the consumer by providing   358
a reasonably accessible, clear, and conspicuously posted privacy   359
policy.   360

    (C)(1) The privacy policy shall include all of the   361
following: 362

    (a) The identity and the contact information of the   363
business, including the business's contact for privacy and data   364
security inquiries, and the identity of any affiliate to which   365
personal data may be transferred by the business;   366

    (b) The categories of personal data the business   367
processes;   368

    (c) The purposes of processing for each category of   369
personal data;   370

    (d) The categories of sources from which the personal data   371
is collected;   372

    (e) The categories of processors with whom the business   373
discloses personal data;   374

    (f) If the business sells personal data to third parties,   375
the business shall clearly and conspicuously disclose such   376
processing, as well as the categories of third parties to whom   377
the business sells personal data, and how a consumer may   378
exercise the right to opt out of such processing;   379

(g) A description of the business's data retention 380

practices for personal data and the purposes for such retention; 381

(h) How individuals can exercise their rights under this 382

chapter; 383

(i) The effective date of the privacy policy; 384

(j) A description of the mechanism or mechanisms a 385

business can use to notify consumers, pursuant to division (E) 386

of this section, when it makes a material change to its privacy 387

policy or decides to process personal data for purposes 388

incompatible with the privacy policy. 389

(2)(a) The privacy policy shall also disclose any and all 390

purposes for which the company collects or processes personal 391

data. 392

(b) Failure on the part of a business to maintain a 393

privacy policy that reflects the business's data privacy 394

practices to a reasonable degree of accuracy shall be considered 395

an unfair and deceptive practice under Chapter 1345. of the 396

Revised Code, except that a consumer shall not be entitled to a 397

private cause of action under that chapter for a failure to 398

comply with division (C)(2)(a) of this section. 399

(D) A business, a co-business, or a processor may provide 400

the privacy policy to the consumer. 401

(E) If a business makes a material change to its privacy 402

policy or decides to process personal data for purposes 403

incompatible with the privacy policy, it shall do either of the 404

following prior to further processing previously collected 405

personal data: 406

(1) Obtain affirmative consent from the consumers 407

affected; | 408

(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. | 409 410 411 412

(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. | 413 414 415 416

(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. | 417 418 419 420

Sec. 1357.04. (A) A consumer, or the parent or guardian of a known child on the child's behalf, may invoke the rights provided under sections 1357.05 to 1357.08 of the Revised Code at any time by making a verifiable request as described in this section. | 421 422 423 424 425

(B)(1)(a) A business shall provide at least one of the following methods for consumers to make requests under sections 1357.05 to 1357.08 of the Revised Code: | 426 427 428

(i) A toll-free telephone number; | 429

(ii) An electronic mail address; | 430

(iii) A web form; | 431

(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 sections 1357.05 to 1357.08 of the Revised Code. | 432 433 434 435

(b) If the consumer maintains an account with the   436
business, the business may require the consumer to submit the   437
request through that account. If the consumer does not maintain   438
an account, the business shall not require that an account be   439
created to submit the request.   440

(2) A business shall reasonably verify the identity of the   441
consumer before granting a request made under sections 1357.05   442
to 1357.08 of the Revised Code.   443

(3) A business need not respond to a consumer request made   444
pursuant to this section if the business is unable to reasonably   445
verify the consumer.   446

(C)(1) A business shall comply with a verified request   447
within forty-five calendar days of the request.   448

(2)(a) For reasonable cause, and upon notice to the   449
consumer citing the cause for the delay, a business may extend   450
the time required to respond to a request under this section by   451
an additional forty-five calendar days.   452

(b) Such a delay shall not be used more than one time per   453
request.   454

(D) Upon receipt of a request made pursuant to sections   455
1357.04 to 1357.08 of the Revised Code, a business shall comply   456
with all requirements of this chapter as they relate to the   457
request, including by notifying the necessary processors.   458

Sec. 1357.05. (A) A consumer may request a copy of the   459
consumer's personal data that the consumer previously provided   460
to the business electronically in a portable, and, to the extent   461
technically feasible, readily usable format.   462

(B) Upon receiving a verified request, a business shall   463

disclose both of the following to the consumer in question in conformance with this section: 464 465

(1) The categories of third parties to whom the business sells personal data, or if it does not sell personal data, that fact; 466 467 468

(2) The personal data the business has collected about the consumer or an accurate description or summary of such data. 469 470

(C) The disclosure shall cover the twelve-month period preceding the business's receipt of the request. 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. 471 472 473 474 475 476

(D) 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. 477 478 479 480

Sec. 1357.06. (A) 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. 481 482 483 484 485 486

(B) Upon receiving a verified request, a business shall 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. 487 488 489 490

Sec. 1357.07. (A) A consumer has the right to request that a business delete personal data that the business has collected 491 492

from the consumer and that the business maintains in an electronic format. 493 494

(B) Such a verifiable request shall reasonably describe the personal data the consumer is requesting be deleted. 495 496

(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 other purpose. 497 498 499 500 501 502

(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. 503 504 505 506 507 508

(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. 509 510 511 512

(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 processor to maintain the consumer's personal data in order to adhere to its written records retention schedule. 513 514 515 516 517

Sec. 1357.08. (A) A consumer has a right to request both of the following from a business: 518 519

(1) That the business not sell the consumer's personal data; 520 521

(2) That the business not process the consumer's personal 522
data for the purpose of targeted advertising. 523

(B) Upon receipt of a verified request made under division 524
(A) of this section, a business shall not sell the personal data 525
of the consumer in question or process the data for the purpose 526
of targeted advertising. 527

(C) A business shall not sell the personal data collected 528
online of a known child without complying with the requirements 529
of or exceptions in the "Children's Online Privacy Protection 530
Act of 1998," 15 U.S.C. 6501, et seq. and its regulations. 531

(D) A business that sells personal data or uses processed 532
personal data for the purposes of targeted advertising shall 533
provide clear and conspicuous notice of these facts in such a 534
manner as to enable a consumer to opt out of the sale of the 535
consumer's personal data, the use of that data for targeted 536
advertising, or both; such as by providing clear and conspicuous 537
notice on its web site privacy policy or other publicly 538
available notice. 539

(E) A business is not required to comply with an opt-out 540
request that the business reasonably determines to be 541
fraudulent. 542

(F) A business shall reasonably inform its processors or 543
third parties of a consumer's request to opt out and request 544
that they comply with the consumer's opt-out request. 545

Sec. 1357.09. (A) Subject to divisions (B) and (C) of this 546
section, a business shall not discriminate against a consumer 547
for exercising the rights provided to a consumer under this 548
chapter. 549

(B) A business may charge different prices or rates for 550

goods or services for individuals who exercise their rights 551

under this chapter for legitimate business reasons or as 552

otherwise permitted or required by applicable law. 553

(C) A business's denial of a consumer's request in 554

compliance with this chapter shall not be considered 555

discrimination against the consumer. 556

(D) Nothing in this section shall be construed as doing 557

either of the following: 558

(1) Requiring a business to provide a product or service 559

that requires the personal data of a consumer that the business 560

does not collect or maintain or requiring a business to provide 561

a product or service if the consumer has exercised the right to 562

opt-out pursuant to section 1357.08 of the Revised Code; 563

(2) Prohibiting a business from offering a different 564

price, rate, level, quality, or selection of goods or services 565

to a consumer, including offering goods or services for no fee, 566

if the offer is related to a consumer's voluntary participation 567

in a bona fide loyalty, rewards, premium features, discounts, or 568

club card program. 569

Sec. 1357.10. (A) A contract between a business and a 570

processor shall govern the data processing procedures of the 571

processor with respect to processing performed on behalf of the 572

business. 573

(B) A processor shall do all of the following: 574

(1) Taking into account the nature of the processing, 575

assist a business, to the extent reasonably possible and through 576

the use of appropriate technical and organizational measures, in 577

fulfilling the obligation of the business to respond to consumer 578

requests made pursuant to sections 1357.04 to 1357.08 of the 579

Revised Code; 580

(2) 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 shall reflect the nature and scope of the activities of the processor and its role in processing the personal data. 581 582 583 584 585 586

(3) At the direction of the business and pursuant to the contract described in division (A) of this section, delete or return, except as required by law, all personal data to the business as requested at the end of the contract period; 587 588 589 590

(4) 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. 591 592 593 594

(C) 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. 595 596 597 598 599 600

Sec. 1357.11. (A) The attorney general has exclusive authority to enforce this chapter. 601 602

(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 or processor has engaged or is engaging in an act or practice that violates this chapter, the attorney general may investigate in accordance with section 603 604 605 606 607 608

1345.06 of the Revised Code.   609

(1) References to "person" in section 1345.06 of the   610
Revised Code shall be interpreted, for purposes of   611
investigations entered into under this section, as referring to   612
an individual or a business.   613

(2) References to a "supplier" in section 1345.06 of the   614
Revised Code shall be interpreted, for purposes of   615
investigations entered into under this section, as referring to   616
a business.   617

(3) Division (E) of section 1345.06 of the Revised Code   618
does not apply to investigations entered into under this   619
section.   620

(4) Nothing in this section shall be construed as granting   621
any additional rights or responsibilities under any other   622
section of Chapter 1345. of the Revised Code.   623

(C) The attorney general shall not disclose publicly the   624
identity of a business or processor investigated under this   625
section or the facts developed in investigations unless either   626
of the following are met: 627

(1) These matters have become a matter of public record in   628
enforcement proceedings, including if the business has entered   629
into an assurance of voluntary compliance with the attorney   630
general pursuant to section 1345.06 of the Revised Code.   631

(2) The business or processor that is the subject of the   632
investigation has consented in writing to public disclosure.   633

(D)(1) If the attorney general, by the attorney general's   634
own inquiries or as a result of complaints, has reasonable cause   635
to believe that a business or processor has engaged or is   636

engaging in an act or practice that violates this chapter, the 637
attorney general, subject to divisions (D)(2) to (4) of this 638
section, may bring an action in a court of common pleas of this 639
state seeking any or all of the following relief: 640

(a) Declaratory judgment that the act or practice violates 641
this chapter; 642

(b) Injunctive relief, including preliminary and permanent 643
injunctions, to prevent further violations of and compel 644
compliance with this chapter; 645

(c) Civil penalties described in division (D)(2)(c) of 646
this section; 647

(d) Attorneys' fees and investigative costs; 648

(e) Any other relief the court determines appropriate, 649
including relief described in division (D)(4) of this section. 650

(2)(a) Prior to initiating any action under this section, 651
the attorney general shall provide a business or processor 652
thirty-days' notice, in writing, identifying the specific 653
provisions of this chapter the attorney general alleges have 654
been or are being violated. 655

(b) If, within the thirty-day period, the business or 656
processor cures the noticed violation and provides the attorney 657
general an express written statement that the alleged violations 658
have been cured and that no further such violations will occur, 659
the attorney general shall not initiate an action against the 660
business or processor, except as provided in division (D)(2)(c) 661
of this section. 662

(c) If a business or processor continues to violate a 663
representation made in such written statement following the cure 664

period described in division (D)(2)(b) of this section or 665
breaches an express written statement provided to the attorney 666
general pursuant to that division, the attorney general may 667
initiate an action pursuant to division (D)(1) of this section 668
and seek civil penalties of up to five thousand dollars for each 669
violation under this chapter. 670

(3) Civil penalties levied in accordance with this 671
division shall be made in accordance with the following 672
criteria: 673

(a) Each provision of this chapter that was violated 674
counts as a separate violation. 675

(b) Each consumer affected counts as a separate violation. 676

(c) When calculating civil penalties, the court may 677
consider all of the following: 678

(i) The number of affected consumers; 679

(ii) The severity of the violation; 680

(iii) The size, nature, and complexity of the business; 681

(iv) The sensitivity of the information in question; 682

(v) The precautions taken to prevent a violation. 683

(4)(a) The court may award relief to each identified 684
consumer affected by a violation of a section of this chapter, 685
regardless of whether any actual damages were suffered, in an 686
amount that is not less than one hundred dollars and not more 687
than seven hundred fifty dollars per violation. 688

(b) If the court finds the business or processor willfully 689
or knowingly violated this chapter, the court may, in its 690
discretion, triple the award. 691

(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) A business or processor that discloses personal data
to another business or processor shall not be liable under this
chapter if the recipient uses it in violation of the
restrictions set forth in this chapter, 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.

(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 does both of the following:

(i) 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

692
693
694
695
696

697
698
699
700

701
702
703
704

705
706
707
708
709
710
711

712
713
714
715

716
717
718
719
720

national institute of standards and technology and referenced by   721
the national institute of standards and technology privacy   722
framework;   723

(ii) Provides individuals with the substantive rights   724
provided to individuals by this chapter.   725

(b) When a final revision to the national institute of   726
standards and technology privacy framework is published, a   727
business shall reasonably conform its privacy program to the   728
revised framework not later than one year after the publication   729
date stated in the revision.   730

(2) The scale and scope of a business's privacy program   731
under division (I)(1) of this section is appropriate if it is   732
based on all of the following factors: 733

(a) The size and complexity of the business;   734

(b) The nature and scope of the activities of the   735
business;   736

(c) The sensitivity of the personal information processed;   737

(d) The cost and availability of tools to improve privacy   738
protections and data governance;   739

(e) Compliance with any comparable state or federal law.   740

(3) A business that satisfies divisions (I)(1) and (2) of   741
this section has an affirmative defense to any cause of action   742
brought under the laws of this state or in the courts of this   743
state that alleges a violation of this chapter or similar claim   744
based on a violation of privacy rights afforded to individuals   745
under this chapter or under Chapter 1345. of the Revised Code,   746
commonly referred to as the consumer sales practices act.   747

(J) Where more than one business or processor, or both a business and a processor, involved in the same processing violate this chapter, liability shall be apportioned according to the amount of responsibility born by each.

(K) The intent of the general assembly in enacting this chapter is 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 as defined in section 2744.01 of the Revised Code shall regulate the collection, processing, or sale of personal data by a business.

Section 2. That existing section 1345.51 of the Revised Code is hereby repealed.

Section 3. The Attorney General may use $250,000 of appropriation item 055321, Operating Expenses, in fiscal year 2025 for the purpose of enforcing the Ohio Personal Privacy Act and enacted sections 1357.01 to 1357.11 of the Revised Code.

Section 4. Sections 1, 2, and 3 of this act take effect one year after the effective date of this section.