———

A BILL

To amend section 1345.51 and to enact sections	1
1355.01, 1355.02, 1355.03, 1355.04, 1355.05,	2
1355.06, 1355.07, 1355.08, 1355.09, 1355.10, and	3
1355.11 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
1355.01, 1355.02, 1355.03, 1355.04, 1355.05, 1355.06, 1355.07,	7
1355.08, 1355.09, 1355.10, and 1355.11 of the Revised Code be	8
enacted to read as follows:	9
Sec. 1345.51. (A) There is hereby created in the state	10
treasury the consumer protection enforcement fund. The fund	11
shall include ~~civil~~ all of the following:	12
(1) Civil 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~~;	15
(2) All civil penalties assessed under division (A) of	16
section 1349.192 of the Revised Code~~, all~~;	17

(3) All moneys awarded under section 1355.11 of the Revised Code other than amounts awarded pursuant to division (D) (4) of that section;   18 19 20

(4) All costs awarded to the attorney general and all penalties imposed under section 4549.48 of the Revised Code, and all;   21 22 23

(5) All money unclaimed under section 4549.50 of the Revised Code.   24 25

(B) The money in the consumer protection enforcement fund shall be used for the sole purpose of paying expenses incurred by the consumer protection section of the office of the attorney general.   26 27 28 29

Sec. 1355.01. As used in this chapter: 30

(A)(1) "Affiliate" means a legal entity that controls, is controlled by, shares common branding with, or is under common control with, another legal entity.   31 32 33

(2) For purposes of division (A)(1) of this section, "control" or "controlled" means a relationship between two legal entities characterized by any of the following: 34 35 36

(a) One entity having ownership of, or the power to vote, more than fifty per cent of the outstanding shares of any class of voting security of the other legal entity;   37 38 39

(b) One entity having control in any manner over the election of a majority of the directors, or of individuals exercising similar functions, of the other entity;   40 41 42

(c) One entity having the power to exercise a controlling influence over the management of the other entity.   43 44

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

(C) "Business" means any limited liability company, limited liability partnership, corporation, sole proprietorship, association, or other group, however organized and regardless of whether operating for profit or not for profit, including a financial institution organized, chartered, or holding a license authorizing operation under the laws of this state, any other state, the United States, or any other country, that, alone or jointly with others, determines the purpose and means of processing personal data. "Business" does not include a public entity, including a political subdivision of this state, a city, township, county, or a processor to the extent that the processor is acting in the role of a processor.

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

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

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

(2) Any third party.

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

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

this state acting only in an individual or household context. 74

"Consumer" does not include a natural person acting in a 75

business capacity or employment context, including contractors, 76

job applicants, officers, directors, or owners. 77

(H) "Deidentified data" means personal data that has been 78

deidentified using commercially reasonable methods such that a 79

consumer, or a device linked to a consumer, cannot be reasonably 80

identified. 81

(I) "HIPAA" has the same meaning as in section 3965.01 of 82

the Revised Code. 83

(J) "Personal data" means any information that is linked 84

or reasonably linkable to an identified or identifiable consumer 85

and that is processed by a business for a commercial purpose. 86

"Personal data" does not include either of the following: 87

(1) Any such data processed from publicly available 88

sources; 89

(2) Pseudonymized, deidentified, or aggregate data. 90

(K) "Process" or "processing" means any operation or set 91

of operations that are performed on personal data, whether or 92

not by automated means, including the collection, use, storage, 93

disclosure, analysis, deletion, transfer, or modification of 94

personal data. 95

(L) "Processor" means a natural or legal person who 96

processes personal data on behalf of a business subject to this 97

chapter. 98

(M) "Pseudonymized or pseudonymous data" means data that 99

no longer allows the identification of an individual without 100

combining it with other information, provided that such 101

additional information is kept separately and is subject to   102

appropriate technical and organizational measures to ensure that   103

the personal data is not attributed to an identified or   104

identifiable consumer.   105

(N) "Publicly available information" means information   106

that is lawfully made available from federal, state, or local   107

government records. "Publicly available information" includes   108

widely available media.   109

(O)(1) "Sale," "sell," or "sold" means the exchange of   110

personal data for monetary or other valuable consideration by a   111

business to a third party.   112

(2) "Sale," "sell," or "sold" does not include any of the   113

following: 114

(a) The disclosure of personal data to a processor who   115

processes the personal data on behalf of a business;   116

(b) The disclosure of personal data to a third party for   117

purposes of providing a product or service requested by the   118

consumer;   119

(c) The disclosure of personal data from one business to   120

another business without monetary or other valuable   121

consideration;   122

(d) The disclosure or transfer of personal data to an   123

affiliate of the business;   124

(e) The disclosure of information that a consumer   125

intentionally made available to the general public via a channel   126

of mass media and did not restrict to a specific audience;   127

(f) The disclosure or transfer of personal data to a third   128

party as an asset that is part of a merger, acquisition,   129

bankruptcy, or other transaction in which the third party   130
assumes control of all or part of the business's assets.   131

    (P) "Targeted advertising" means displaying to a consumer   132
an advertisement that is selected based on personal data   133
obtained or inferred over time from the consumer's activities   134
across nonaffiliated web sites, applications, or online services   135
to predict consumer preferences or interests. "Targeted   136
advertising" does not include any of the following: 137

    (1) Advertising to a consumer in response to the   138
consumer's request for information or feedback;   139

    (2) Advertisements based on activities within a business's   140
or processor's own web sites or online applications;   141

    (3) Advertisements based on the context of a consumer's   142
current search query, visit to a web site, or online   143
application;   144

    (4) Processing personal data solely for measuring or   145
reporting advertising performance, reach, or frequency.   146

    (Q) "Third party" means a natural or legal person, public   147
authority, agency, or body other than the consumer, business, or   148
processor, or an affiliate of the business or processor.   149

    (R) "Verified request" means a request submitted to a   150
business under sections 1355.03 to 1355.06 of the Revised Code   151
that has been verified by the business as being made by the   152
consumer in question or by the consumer's representative.   153

    As used in division (R) of this section, "consumer's   154
representative" means a child's parent or a representative of a   155
person for whom a guardian of the estate or conservator has been   156
appointed.   157

Sec. 1355.02. (A) This chapter applies to businesses that 158

conduct business in this state, or produce products or services 159

targeted to consumers in this state, that satisfy one or more of 160

the following criteria: 161

(1) The business's annual gross revenues generated in this 162

state exceed twenty-five million dollars; 163

(2) During a calendar year, the business controls or 164

processes personal data of one hundred thousand or more 165

consumers; 166

(3) During a calendar year, the business derives over 167

fifty per cent of its gross revenue from the sale of personal 168

data and processes or controls personal data of twenty-five 169

thousand or more consumers. 170

(B) This chapter does not apply to any of the following: 171

(1) Any body, authority, board, bureau, commission, 172

district, or agency of this state or of any political 173

subdivision of this state; 174

(2) A financial institution, data, or an affiliate of a 175

financial institution governed by Title V of the federal "Gramm- 176

Leach-Bliley Act," 15 U.S.C. 6801 et seq. and related 177

regulations; 178

(3) A covered entity or business associate governed by the 179

privacy, security, and breach notification rules issued by the 180

United States department of health and human services, 45 C.F.R. 181

Parts 160 and 164 established pursuant to HIPAA, and the health 182

information technology for economic and clinical health act, 42 183

U.S.C. 300jj et seq; 184

(4) An institution of higher education. 185

(5) Business to business transactions.   186

(6) Any of the following: 187

(a) Any insurer or independent insurance agent, as defined   188
in section 3905.49 of the Revised Code;   189

(b) Any nonprofit organization established to detect or   190
prevent insurance-related crime or fraud;   191

(c) Any advisory organization described in section 3937.09   192
of the Revised Code;   193

(d) Any rating organization licensed pursuant to section   194
3937.05 of the Revised Code or an affiliate thereof.   195

(7) Personal data regulated by the federal "Children's   196
Online Privacy Protection Act," 15 U.S.C. 6501 to 6506, if   197
collected, processed, and maintained in compliance with that law 198
and its implementing regulations or exemptions.   199

(C) The following information and data are exempt from   200
this chapter: 201

(1) Protected health information under HIPAA;   202

(2) Health records, as described in Chapter 3798. of the   203
Revised Code;   204

(3) Patient identifying information for purposes of 42   205
U.S.C. 290dd-2;   206

(4) Any of the following types of information or data: 207

(a) Identifiable private information for purposes of the   208
federal policy for the protection of human subjects under 45   209
C.F.R. Part 46;   210

(b) Identifiable private information that is otherwise   211

information collected as part of human subjects research 212

pursuant to the good clinical practice guidelines issued by the 213

international council for harmonisation of technical 214

requirements for pharmaceuticals for human use; 215

(c) Data related to the protection of human subjects under 216

21 C.F.R. parts 6, 50, and 56, or personal data used or shared 217

in research conducted in accordance with the requirements set 218

forth in this chapter, or other research conducted in accordance 219

with applicable law. 220

(5) Information and documents created for purposes of the 221

federal "Health Care Quality Improvement Act of 1986," 42 U.S.C. 222

11101 et seq.; 223

(6) Patient safety work product for purposes of the 224

federal "Patient Safety and Quality Improvement Act," 42 U.S.C. 225

299b-21 et seq.; 226

(7) Information derived from any of the health care- 227

related information listed in division (C) of this section that 228

is deidentified in accordance with the requirements for 229

deidentification pursuant to HIPAA; 230

(8) Information originating from, and intermingled to be 231

indistinguishable with, or information treated in the same 232

manner as information exempt under division (C) of this section 233

that is maintained by a covered entity or business associate as 234

defined by HIPAA or a program or a qualified service 235

organization as defined by 42 U.S.C. 290dd-2; 236

(9) Information used only for public health activities and 237

purposes as authorized by HIPAA; 238

(10) The collection, maintenance, disclosure, sale, 239

communication, or use of any personal information bearing on a 240

consumer's credit worthiness, credit standing, credit capacity,   241

character, general reputation, personal characteristics, or mode   242

of living by a consumer reporting agency or furnisher that   243

provides information for use in a consumer report, and by a user   244

of a consumer report, but only to the extent that such activity   245

is regulated by and authorized under the federal "Fair Credit   246

Reporting Act," 15 U.S.C. 1681 et seq.;   247

(11) Personal data collected, processed, sold, or   248

disclosed in compliance with the federal "Driver's Privacy   249

Protection Act of 1994," 18 U.S.C. 2721 et seq.;   250

(12) Personal data regulated by the federal "Family   251

Educational Rights and Privacy Act," 20 U.S.C. 1232g et seq.;   252

(13) Personal data collected, processed, sold, or   253

disclosed in compliance with the federal "Farm Credit Act," 12   254

U.S.C. 2001 et seq.;   255

(14) Data processed or maintained in accordance with any   256

of the following: 257

(a) In the course of an individual applying to, employed   258

by, or acting as an agent or independent contractor of a   259

business subject to this chapter, processor, or a related third   260

party, to the extent that the data is collected and used within   261

the context of that role;   262

(b) For emergency contact purposes for individuals   263

described in division (C)(14)(a) of this section;   264

(c) As necessary to administer employment benefits to   265

those individuals described in division (C)(14)(a) of this   266

section, as well as to any persons related to those individuals,   267

such as dependents or spouses.   268

(D) This chapter does not apply to the extent necessary 269
for a business or processor to do any of the following: 270

(1) Comply with federal or state law; 271

(2) Comply with a civil, criminal, or regulatory inquiry, 272
investigation, subpoena, or summons by federal, state, or local 273
authorities; 274

(3) Cooperate with law enforcement agencies concerning 275
conduct or activity that the business, the processor, or a third 276
party reasonably and in good faith believes may violate federal, 277
state, or local law; 278

(4) Exercise, or defend against, legal claims; 279

(5)(a) Prevent, detect, or protect against, or provide a 280
response to, security incidents, identity theft, fraud, 281
harassment, malicious or deceptive activities, or any illegal 282
activity; 283

(b) Report or prosecute those responsible for any such 284
action. 285

(6) Preserve the integrity or security of systems; 286

(7) Engage in public or peer-reviewed scientific, 287
historical, or statistical research in the public interest that 288
adheres to all other applicable ethics and privacy laws, if the 289
deletion of the information is likely to render impossible or 290
seriously impair the achievement of the research and the 291
consumer in question has provided consent; 292

(8) Assist another business, processor, or third party 293
with any of the obligations imposed under division (C) of this 294
section; 295

(9) Provide a product or service specifically requested by a consumer or a child's parent or guardian; 296 297

(10) Perform a contract to which a consumer or child's parent or guardian is a party, including fulfilling the terms of a written warranty; 298 299 300

(11) Comply with the request of a consumer or child's parent or guardian prior to entering into a contract; 301 302

(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. 303 304 305 306

(E) The requirements of this chapter do not apply to the extent that compliance would violate or hinder an evidentiary privilege under Ohio law. 307 308 309

(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: 310 311 312 313

(1) Conduct internal research solely to improve or repair products, services, or technology; 314 315

(2) Identify and repair technical errors that impair existing or intended functionality; 316 317

(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 318 319 320 321 322 323

the consumer is a party; 324

(4) Effectuate a product recall. 325

(G) This chapter shall not be construed as requiring a 326
business or processor to collect personal data that it would not 327
otherwise collect in the ordinary course of its business, retain 328
personal data for longer than it would otherwise retain such 329
data in the ordinary course of its business, or reidentify or 330
otherwise link information that is not maintained in a manner 331
that would be considered personal data. 332

(H) Obligations imposed on businesses and processors under 333
this chapter shall not be construed as doing either of the 334
following: 335

(1) Adversely affecting the rights or freedoms of any 336
persons, such as exercising the right of free speech pursuant to 337
the first amendment of the United States Constitution or Article 338
I, Section 11, of the Ohio Constitution; 339

(2) Applying to the processing of personal data by a 340
natural person in the course of a purely personal or household 341
activity. 342

(I) The consumer rights provided under sections 1355.04 to 343
1355.08 of the Revised Code do not apply to pseudonymous data in 344
cases where the business or processor is able to demonstrate 345
that any information necessary to identify the consumer is kept 346
separately and is subject to effective technical and 347
organizational controls to prevent the business or processor 348
from accessing such information. 349

(J) Nothing in this chapter requires a business or 350
processor to disclose a trade secret. 351

Sec. 1355.03. (A) A consumer has a right to know the   352
personal data that a business collects about that consumer, such   353
as by obtaining a privacy policy from the business.   354

(B) A business shall provide consumers notice about the   355
personal data that it processes about the consumer by providing   356
a reasonably accessible, clear, and conspicuously posted privacy   357
policy.   358

(C)(1) The privacy policy shall include all of the   359
following: 360

(a) The identity and the contact information of the   361
business, including the business's contact for privacy and data   362
security inquiries, and the identity of any affiliate to which   363
personal data may be transferred by the business;   364

(b) The categories of personal data the business   365
processes;   366

(c) The purposes of processing for each category of   367
personal data;   368

(d) The categories of sources from which the personal data   369
is collected;   370

(e) The categories of processors with whom the business   371
discloses personal data;   372

(f) If the business sells personal data to third parties,   373
the business shall clearly and conspicuously disclose such   374
processing, as well as the categories of third parties to whom   375
the business sells personal data, and how a consumer may   376
exercise the right to opt out of such processing;   377

(g) A description of the business's data retention   378
practices for personal data and the purposes for such retention;   379

(h) How individuals can exercise their rights under this 380
chapter; 381

(i) The effective date of the privacy policy; 382

(j) A description of the mechanism or mechanisms a 383
business can use to notify consumers, pursuant to division (E) 384
of this section, when it makes a material change to its privacy 385
policy or decides to process personal data for purposes 386
incompatible with the privacy policy. 387

(2)(a) The privacy policy shall also disclose any and all 388
commercial purposes for which the company collects or processes 389
personal data. 390

(b) Failure on the part of a business to maintain a 391
privacy policy that reflects the business's data privacy 392
practices to a reasonable degree of accuracy shall be considered 393
an unfair and deceptive practice under Chapter 1345. of the 394
Revised Code, except that a consumer shall not be entitled to a 395
private cause of action under that chapter for a failure to 396
comply with division (C)(2)(a) of this section. 397

(D) A business, a co-business, or a processor may provide 398
the privacy policy to the consumer. 399

(E) If a business makes a material change to its privacy 400
policy or decides to process personal data for purposes 401
incompatible with the privacy policy, it shall do either of the 402
following prior to further processing previously collected 403
personal data: 404

(1) Obtain affirmative consent from the consumers 405
affected; 406

(2)(a) Provide notice outlining the changes to the 407

business's privacy policy and providing affected consumers a 408

reasonable means to opt out of having their data processed or 409

disseminated. 410

(b) Such notice shall be provided not less than sixty days 411

prior to implementing the change, taking into account available 412

technology and the nature of the relationship between the 413

business and the consumer. 414

(F) The business shall provide direct notification, where 415

possible, regarding a material change to the privacy policy to 416

affected consumers, taking into account available technology and 417

the nature of the relationship. 418

Sec. 1355.04. (A) A consumer, or the parent or guardian of 419

a known child on the child's behalf, may invoke the rights 420

provided under sections 1355.05 to 1355.08 of the Revised Code 421

at any time by making a verifiable request as described in this 422

section. 423

(B)(1)(a) A business shall provide at least one of the 424

following methods for consumers to make requests under sections 425

1355.05 to 1355.08 of the Revised Code: 426

(i) A toll-free telephone number; 427

(ii) An electronic mail address; 428

(iii) A web form; 429

(iv) A clear and conspicuous link on the business's main 430

internet homepage to an internet web page that enables a 431

consumer to exercise the rights provided under sections 1355.05 432

to 1355.08 of the Revised Code. 433

(b) However, if the consumer maintains an account with the 434

business, the business may require the consumer to submit the 435

request through that account. If the consumer does not maintain   436
an account, the business shall not require that an account be   437
created to submit the request.   438

    (2) A business shall reasonably verify the identity of the   439
consumer before granting a request made under sections 1355.05   440
to 1355.08 of the Revised Code.   441

    (3) A business need not respond to a consumer request made   442
pursuant to this section if the business is unable to reasonably   443
verify the consumer.   444

    (C)(1) A business shall comply with a verified request   445
within forty-five calendar days of the request.   446

    (2)(a) For reasonable cause, and upon notice to the   447
consumer citing the cause for the delay, a business may extend   448
the time required to respond to a request under this section by   449
an additional forty-five calendar days.   450

    (b) Such a delay shall not be used more than one time per   451
request.   452

    (D) Upon receipt of a request made pursuant to sections   453
1355.04 to 1355.08 of the Revised Code, a business shall comply   454
with all requirements of this chapter as they relate to the   455
request, including by notifying the necessary processors.   456

    Sec. 1355.05. (A) A consumer may request a copy of the   457
consumer's personal data that the consumer previously provided   458
to the business electronically in a portable, and, to the extent   459
technically feasible, readily usable format.   460

    (B) Upon receiving a verified request, a business shall   461
disclose both of the following to the consumer in question in   462
conformance with this section: 463

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

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

(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.

(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.

Sec. 1355.06. (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.

(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.

Sec. 1355.07. (A) A consumer shall have the right to request that a business delete personal data that the business has collected from the consumer for commercial purposes and that the business maintains in an electronic format.

464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492

(B) Such a verifiable request shall reasonably describe   493
the personal data the consumer is requesting be deleted.   494

(C)(1) If the consumer's personal data is stored on   495
archived or backup systems, the business may delay compliance   496
with the consumer's request to delete until the archived or   497
backup system relating to that data is restored to an active   498
system, next accessed, or used for a sale, disclosure, or   499
commercial purpose.   500

(2) If the consumer's personal data is stored on archived   501
or backup systems, the business may comply with the consumer's   502
request by deleting or overwriting the data in accordance with a   503
scheduled backup or creation of a new archive, so long as the   504
business employs encryption standards to protect that data both   505
when the data is in transit and is at rest.   506

(D) A business is not required to delete personal data   507
that it maintains or uses as aggregated, deidentified, or   508
pseudonymous data, provided that such data in the possession of   509
the business is not linked to a specific consumer.   510

(E) A business, or an associated processor, shall not be   511
required to comply with a consumer's request to delete personal   512
data if it is necessary for the business or processor to   513
maintain the consumer's personal data in order to adhere to its   514
written records retention schedule.   515

   Sec. 1355.08. (A) A consumer has a right to request both   516
of the following from a business: 517

(1) That the business not sell the consumer's personal   518
data;   519

(2) That the business not process the consumer's personal   520
data for the purpose of targeted advertising.   521

(B) Upon receipt of a verified request made under division   522

(A) of this section, a business shall not sell the personal data   523

of the consumer in question or process the data for the purpose   524

of targeted advertising.   525

(C) A business shall not sell the personal data collected   526

online of a known child without complying with the requirements   527

of or exceptions in the "Children's Online Privacy Protection   528

Act of 1998," 15 U.S.C. 6501, et seq. and its regulations.   529

(D) A business that sells personal data or uses processed   530

personal data for the purposes of targeted advertising shall   531

provide clear and conspicuous notice of these facts in such a   532

manner as to enable a consumer to opt out of the sale of the   533

consumer's personal data, the use of that data for targeted   534

advertising, or both; such as by providing clear and conspicuous   535

notice on its web site privacy policy or other publicly   536

available notice.   537

(E) A business is not required to comply with an opt-out   538

request that the business reasonably determines to be   539

fraudulent.   540

(F) A business shall reasonably inform its processors or   541

third parties of a consumer's request to opt out and request   542

that they comply with the consumer's opt-out request.   543

   Sec. 1355.09. (A) Subject to divisions (B) and (C) of this   544

section, a business shall not discriminate against a consumer   545

for exercising the rights provided to a consumer under this   546

chapter.   547

(B) A business may charge different prices or rates for   548

goods or services for individuals who exercise their rights   549

under this chapter for legitimate business reasons or as   550

otherwise permitted or required by applicable law.   551

(C) A business's denial of a consumer's request in   552
compliance with this chapter shall not be considered   553
discrimination against the consumer.   554

(D) Nothing in this section shall be construed as doing   555
either of the following: 556

(1) Requiring a business to provide a product or service   557
that requires the personal data of a consumer that the business   558
does not collect or maintain or requiring a business to provide   559
a product or service if the consumer has exercised the right to   560
opt-out pursuant to section 1355.08 of the Revised Code;   561

(2) Prohibiting a business from offering a different   562
price, rate, level, quality, or selection of goods or services   563
to a consumer, including offering goods or services for no fee,   564
if the offer is related to a consumer's voluntary participation   565
in a bona fide loyalty, rewards, premium features, discounts, or   566
club card program.   567

Sec. 1355.10. (A) A contract between a business and a   568
processor shall govern the data processing procedures of the   569
processor with respect to processing performed on behalf of the   570
business.   571

(B) A processor shall do all of the following: 572

(1) Taking into account the nature of the processing,   573
assist a business, to the extent reasonably possible and through   574
the use of appropriate technical and organizational measures, in   575
fulfilling the obligation of the business to respond to consumer   576
requests made pursuant to sections 1355.04 to 1355.08 of the   577
Revised Code;   578

(2) Develop, implement, and maintain reasonable   579
administrative, technical, and physical safeguards to protect   580
the security and confidentiality of personal data processed by   581
the processor. The safeguards shall reflect the nature and scope   582
of the activities of the processor and its role in processing   583
the personal data.   584

(3) At the direction of the business and pursuant to the   585
contract described in division (A) of this section, delete or   586
return, except as required by law, all personal data to the   587
business as requested at the end of the contract period;   588

(4) If the processor uses the services of a subprocessor   589
with respect to a business, require the subprocessor to meet the   590
obligations of the processor with respect to any personal data   591
collected.   592

(C) Whether a person acts as a business or a processor   593
with respect to a specific processing of personal data is a   594
fact-based determination that depends on the context in which   595
the personal data is processed. A processor adhering to the   596
instructions of a business with respect to a specific processing   597
of personal data is considered a processor.   598

Sec. 1355.11. (A) The attorney general has exclusive   599
authority to enforce this chapter.   600

(B) Except as provided in divisions (B)(1) to (4) of this   601
section, if, by the attorney general's own inquiries or as a   602
result of complaints, the attorney general has reasonable cause   603
to believe that a business or processor has engaged or is   604
engaging in an act or practice that violates this chapter, the   605
attorney general may investigate in accordance with section   606
1345.06 of the Revised Code.   607

(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 or processor 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 or processor that is the subject of the
investigation has consented in writing to public disclosure.

(D)(1) If the attorney general, by the attorney general's
own inquiries or as a result of complaints, has reasonable cause
to believe that a business or processor has engaged or is
engaging in an act or practice that violates this chapter, the

608
609
610
611
612

613
614
615
616

617
618
619

620
621
622

623
624
625
626

627
628
629
630

631
632

633
634
635
636

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

(a) Declaratory judgment that the act or practice violates   640
this chapter;   641

(b) Injunctive relief, including preliminary and permanent   642
injunctions, to prevent further violations of and compel   643
compliance with this chapter;   644

(c) Civil penalties described in division (D)(2)(c) of   645
this section;   646

(d) Attorneys' fees and investigative costs;   647

(e) Any other relief the court determines appropriate,   648
including relief described in division (D)(4) of this section.   649

(2)(a) Prior to initiating any action under this section,   650
the attorney general shall provide a business or processor   651
thirty-days' notice, in writing, identifying the specific   652
provisions of this chapter the attorney general alleges have   653
been or are being violated.   654

(b) If, within the thirty-day period, the business or   655
processor cures the noticed violation and provides the attorney   656
general an express written statement that the alleged violations   657
have been cured and that no further such violations will occur,   658
the attorney general shall not initiate an action against the   659
business or processor, except as provided in division (D)(2)(c)   660
of this section.   661

(c) If a business or processor continues to violate a   662
representation made in such written statement following the cure   663
period described in division (D)(2)(b) of this section or   664

breaches an express written statement provided to the attorney 665

general pursuant to that division, the attorney general may 666

initiate an action pursuant to division (D)(1) of this section 667

and seek civil penalties of up to five thousand dollars for each 668

violation under this chapter. 669

(3) Civil penalties levied in accordance with this 670

division shall be made in accordance with the following 671

criteria: 672

(a) Each provision of this chapter that was violated 673

counts as a separate violation. 674

(b) Each consumer affected counts as a separate violation. 675

(c) When calculating civil penalties, the court may 676

consider all of the following: 677

(i) The number of affected consumers; 678

(ii) The severity of the violation; 679

(iii) The size, nature, and complexity of the business; 680

(iv) The sensitivity of the information in question; 681

(v) The precautions taken to prevent a violation. 682

(4)(a) The court may award relief to each identified 683

consumer affected by a violation of a section of this chapter, 684

regardless of whether any actual damages were suffered, in an 685

amount that is not less than one hundred dollars and not more 686

than seven hundred fifty dollars per violation. 687

(b) If the court finds the business or processor willfully 688

or knowingly violated this chapter, the court may, in its 689

discretion, triple the award. 690

(E) Any moneys awarded under this section, with the 691

exception of amounts awarded under division (D)(4) of this   692

section, shall be deposited into the consumer protection   693

enforcement fund established in section 1345.51 of the Revised   694

Code.   695

(F) The remedies available to the attorney general under   696

this section are cumulative and concurrent, and the exercise of   697

one remedy by the attorney general does not preclude or require   698

the exercise of any other remedy.   699

(G) Any violation of this chapter shall not serve as the   700

basis for, or be subject to, a private right of action,   701

including a class action lawsuit, under this chapter or under   702

any other law.   703

(H) A business or processor that discloses personal data   704

to another business or processor shall not be liable under this   705

chapter if the recipient uses it in violation of the   706

restrictions set forth in this chapter, provided that, at the   707

time of disclosing the personal data, the business or processor   708

does not have actual knowledge, or reason to believe, that the   709

processor intends to commit such a violation.   710

(I)(1)(a) A business has an affirmative defense against   711

allegations of violations of this chapter if that business   712

creates, maintains, and complies with a written privacy program   713

that does both of the following: 714

(i) Reasonably conforms to the national institute of   715

standards and technology privacy framework entitled "A Tool for   716

Improving Privacy through Enterprise Risk Management Version   717

1.0," including applicable controls selected by the business   718

from special publication 800-53 and 800-53a published by the   719

national institute of standards and technology and referenced by   720

the national institute of standards and technology privacy 721

framework; 722

(ii) Provides individuals with the substantive rights 723

provided to individuals by this chapter. 724

(b) When a final revision to the national institute of 725

standards and technology privacy framework is published, a 726

business shall reasonably conform its privacy program to the 727

revised framework not later than one year after the publication 728

date stated in the revision. 729

(2) The scale and scope of a business's privacy program 730

under division (I)(1) of this section is appropriate if it is 731

based on all of the following factors: 732

(a) The size and complexity of the business; 733

(b) The nature and scope of the activities of the 734

business; 735

(c) The sensitivity of the personal information processed; 736

(d) The cost and availability of tools to improve privacy 737

protections and data governance; 738

(e) Compliance with any comparable state or federal law. 739

(3) A business that satisfies divisions (I)(1) and (2) of 740

this section has an affirmative defense to any cause of action 741

brought under the laws of this state or in the courts of this 742

state that alleges a violation of this chapter or similar claim 743

based on a violation of privacy rights afforded to individuals 744

under this chapter or under Chapter 1345. of the Revised Code, 745

commonly referred to as the consumer sales practices act. 746

(J) Where more than one business or processor, or both a 747

business and a processor, involved in the same processing 748

violate this chapter, liability shall be apportioned according 749

to the amount of responsibility born by each. 750

(K) The intent of the general assembly in enacting this 751

chapter is to establish a statewide, comprehensive enactment 752

that applies to all parts of the state, operates uniformly 753

throughout the state, and sets forth police regulations. No 754

political subdivision as defined in section 2744.01 of the 755

Revised Code shall regulate the collection, processing, or sale 756

of personal data by a business. 757

Section 2. That existing section 1345.51 of the Revised 758

Code is hereby repealed. 759

Section 3. The Attorney General may use $250,000 of 760

appropriation item 055321, Operating Expenses, in fiscal year 761

2023 for the purpose of enforcing the Ohio Personal Privacy Act 762

and enacted sections 1355.01 to 1355.11 of the Revised Code. 763

Section 4. Sections 1, 2, and 3 of this act take effect 764

one year after the effective date of this section. 765