

Government of the District of Columbia
UNIFORM LAW COMMISSION



October 18, 2021

The Honorable Phil Mendelson
Chairman
Council of the District of Columbia
The John A. Wilson Building,
1350 Pennsylvania Avenue, NW
Washington, DC 20004

RE: Request for introduction of the Uniform Personal Data Protection Act of 2021.

Dear Chairman Mendelson:

Pursuant to Rule 401(b)(1) of the Rules of Organization and Procedure for the Council, this is to request, on behalf of the District of Columbia Uniform Law Commission, that you introduce the proposed “Uniform Personal Data Protection Act of 2021.” This bill is based on the Uniform Personal Data Protection Act (“UPDPA”), which was adopted by the National Conference of Commissioners on Uniform State Laws (“NCCUSL”) in July of this year. UPDPA is the product of several years’ work by NCCUSL with the participation of a broad mixture of organizations and individuals concerned with personal data privacy. UPDPA applies fair information practice principles to the collection and use of personal data from consumers by businesses. It is not regulatory and, thus, avoids the high compliance and enforcement costs and the anticompetitive effects of regulatory acts. It balances the interests of consumers and businesses and permits flexibility and innovation, which will benefit consumers.

One of the inducements for NCCUSL to undertake this project was the threat of federal preemption. A number of bills have been introduced in Congress that would preempt state laws in this area and regulate data practices and consumers’ privacy rights through the Federal Trade Commission. NCCUSL believes that state law should govern areas of the law traditionally governed by state law, such as consumer protection.

UPDPA applies to data controllers, which determine the purpose and means of data processing, and to data processors, which process the data at the direction of the controllers. The act applies to “personal data,” which includes (1) data linked to an individual by a direct identifier, such as name, address, and telephone number, and

(2) pseudonymized data,” which is data that lacks direct identifiers but that can be readily accessed by use of a code, such as an Internet Protocol Address.

UPDPA divides data practices into three categories: (1) compatible data practices—*i.e.*, those that are consistent with the data subject’s interests or reasonable expectations; (2) prohibited data practices—*i.e.*, those that pose substantial risk of harm to data subjects; and (3) incompatible (but consentable) data practices—*i.e.*, those that are neutral as to their benefit or harm and may be used with the consent of the data subject. UPDPA provides special protections for “sensitive data,” including information as to race, religious belief, gender, sexual orientation, citizenship, immigration status, geolocation in real time, criminal record, medical diagnoses, Social Security Number, numbers of government issued identification, and information pertaining to children under 13. An incompatible data practice involving sensitive data may only be used with the express consent of the data user in advance.

UPDPA applies to controllers or processors that conduct business in the District or provide products or services directed to District residents. The Act applies to controllers or processors that “maintain” personal data of more than 50,000 District residents or that earn more than 50% of their annual income from maintaining this data, and also to any such business that maintains data for incompatible or prohibited data practices. To be “maintained,” data must be part of a system of records about individuals for purposes of individualized communication or decisions. Thus, it excludes data transactions used solely for credit card purchases or unstructured e-mail communications. UPDPA does not apply to data maintained by the District, data subject to disclosure by law or court order, data maintained for employment purposes, or publicly available information. The latter exemption is included to avoid challenges under the First Amendment.

UPDPA gives data subjects important, nonwaivable, rights—notably the right a copy of their data and the right to have the collecting controller correct or amend data. UPDPA does not contain a right to deletion of data because, among other reason, this would invite challenges under the First Amendment. It was considered that the restrictions of use of data for compatible practices and for incompatible practices only with consent are sufficient. UPDPA also requires controllers to adopt a clear and accessible data privacy policy, and requires controllers and processors to undertake data privacy security risk assessments.

To avoid unnecessary duplicative enforcement schemes, UPDPA provides that transactions covered by specific federal statutes, including the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act for financial information, and the Children’s Online Privacy Protection Act, are exempted. UPDPA also authorizes the Attorney General for the District of Columbia to determine, on a case-by-case basis, whether transactions subject to laws of other jurisdictions that are at least protective as UPDPA are similarly exempt.

To provide flexibility to respond to unforeseen developments in the future affecting personal data, UPDPA authorizes the creation of “voluntary consensus standards” with the participation of all pertinent stakeholders for an industry. These standards would have to be adopted by the attorneys general of states that have enacted UPDPA and promulgated by rule. UPDPA contemplates that the adoption of these standards will be coordinated by the National Association of Attorneys General, which has a Working Group on Data Privacy, and, thus, will achieve national uniformity. Similar approaches have been taken in other areas of the law, including consumer protect safety and children’s on-line privacy.

UPDPA does not attempt to create its own enforcement scheme, but incorporates the consumer protection procedures of each enacting state. Enforcement of UPDPA would be by the Attorney General for the District of Columbia. It is contemplated that enforcement of data practices of controllers and processors that engage in multistate activities will be coordinated by the state attorneys general.

Finally, UPDPA does not displace general causes of action under statute or the common law, such as those for defamation, invasion of the right of privacy, and intentional infliction of emotional harm. These general rights of action remain intact.

In sum, enactment of UPDPA would provide real protections for consumers’ personal data without imposing onerous, and often impossible, burdens on controllers and processors. It is a law that will encourage the responsible growth of data practices in the District.

The proposed Uniform Personal Data Protection Act of 2021 and a copy of the official version of UPDPA with comments is being filed with the Secretary with this letter. In addition, we have filed (1) a short summary of UPDPA; (2) a statement as to why UPDPA should be adopted, and (3) the official version of the UPDPA with comments. Please let us know if you have any questions.

Sincerely,

A handwritten signature in blue ink that reads "James C. McKay, Jr." The signature is written in a cursive style with a large, looping initial "J".

James C. McKay, Jr.
Chair
D.C. Uniform Law Commission

cc: Uniform Law Commissioners



Chairman Phil Mendelson at the request of the
District of Columbia Uniform Law Commission

A BILL

IN THE COUNCIL OF THE DISTRICT OF COLUMBIA

To enact the Uniform Personal Data Protection Act, to apply fair information practice principles to the collection and use of consumers' personal data by businesses; to permit without consent compatible data practices that are consistent with the data user's general expectations or benefit the data users; to permit incompatible data practices that are not harmful with notice and consent; to prohibit certain data practices that pose a substantial risk of harm; to cover data controllers and processors that conduct business in the District or provide products of services directed toward District residents and maintain personal data of more than 50,000 residents or earn more than 50% of annual income from maintaining this data, or any businesses that maintain incompatible or prohibited data practices; to exempt data maintained by District agencies and certain other data, including publicly available information, data subject to disclosure by court order or statute, and data relating to employment; to give data subjects the right to a copy of, and to the correction or amendment of, their data; to require data controllers to adopt a data privacy policy; to require controllers and processors to conduct appropriate security risk assessments; to provide that compliance with certain federal laws, and laws of other jurisdictions designated by the Attorney General, suffices as compliance with this chapter; to encourage the creation of voluntary consensus standards by stakeholders that are recognized by the Attorney General by rule; to provide for enforcement through existing consumer protection procedures; and to provide that existing common-law causes of action are not displaced by this chapter.

BE IT ENACTED BY THE COUNCIL OF THE DISTRICT OF COLUMBIA, That this act may be cited as the "Uniform Personal Data Protection Act of 2021."

Sec. 2. Subtitle II of Title 28 of the District of Columbia Code is amended as follows:

42 (a) The table of contents is amended by adding a new chapter designation to read as
43 follows:

44 "Chapter 55. Personal Data Protection; Uniform Act".

45 (b) A new Chapter 55 is added to read as follows:

46 "CHAPTER 55. PERSONAL DATA PROTECTION; UNIFORM ACT

47 "Section

48 "28-5501. Title.

49 "28-5502. Definitions.

50 "28-5503. Scope.

51 "28-5504. Controller and processor responsibilities.

52 "28-5505. Right to copy and correct personal data.

53 "28-5506. Privacy policy.

54 "28-5507. Compatible data practice.

55 "28-5508. Incompatible data practice.

56 "28-5509. Prohibited data practice.

57 "28-5510. Data-privacy and security-risk assessment.

58 "28-5511. Compliance with other law protecting personal data.

59 "28-5512. Compliance with voluntary consensus standard.

60 "28-5513. Content of voluntary consensus standard.

61 "28-5514. Procedure for development of voluntary consensus standard.

62 "28-5515. Recognition of voluntary consensus standard.

63 "28-5516. Rules and enforcement.

64 "28-5517. Limits of chapter.

65 “28-5518. Uniformity of application and construction.

66 “28-5519. Electronic Records and Signatures in Global and National Commerce Act.”

67 “§ 28-5501. Title.

68 “This chapter may be cited as the Uniform Personal Data Protection Act.

69 “§ 28-5502. Definitions.

70 “In this chapter:

71 “(1) “Attorney General” means the Attorney General for the District of Columbia.

72 “(2) “Collecting controller” means a controller that collects personal data directly from a
73 data subject.

74 “(3) “Compatible data practice” means processing consistent with § 28-5507.

75 “(4) “Controller” means a person that, alone or with others, determines the purpose and
76 means of processing.

77 “(5) “Data subject” means an individual who is identified or described by personal data.

78 “(6) “Deidentified data” means data that is modified to remove all direct identifiers and to
79 reasonably ensure that the record cannot be linked to an identified data subject by a person that
80 does not have personal knowledge of or special access to the data subject’s information.

81 “(7) “Direct identifier” means information that is commonly used to identify a data
82 subject, including name, physical address, email address, recognizable photograph, and
83 telephone number.

84 “(8) “District” means the District of Columbia.

85 “(9) “Incompatible data practice” means processing that may be performed consistent
86 with § 28-5508.

87 “(10) “Maintains”, with respect to personal data, means to retain, hold, store, or preserve
88 personal data as a system of records used to retrieve records about individual data subjects for
89 the purpose of individualized communication or treatment.

90 “(11) “Person” means an individual, estate, business or nonprofit entity, or other legal
91 entity. The term does not include a public corporation or government or governmental
92 subdivision, agency, or instrumentality.

93 “(12) “Personal data” means a record that identifies or describes a data subject by a direct
94 identifier or is pseudonymized data. The term does not include deidentified data.

95 “(13) “Processing” means performing or directing performance of an operation on
96 personal data, including collection, transmission, use, disclosure, analysis, prediction, and
97 modification of the personal data, whether or not by automated means. “Process” has a
98 corresponding meaning.

99 “(14) “Processor” means a person that processes personal data on behalf of a controller.

100 “(15) “Prohibited data practice” means processing prohibited by § 28-5509.

101 “(16) “Pseudonymized data” means personal data without a direct identifier that can be
102 reasonably linked to a data subject’s identity or is maintained to allow individualized
103 communication with, or treatment of, the data subject. The term includes a record without a
104 direct identifier if the record contains an Internet protocol address, browser, software, or
105 hardware identification code, or other data uniquely linked to a particular device. The term does
106 not include deidentified data.

107 “(17) “Publicly available information” means information:

108 “(A) lawfully made available from a federal, state, or local government record;

109 “(B) available to the general public in widely distributed media, including:

110 “(i) A publicly accessible website;
111 “(ii) A website or other forum with restricted access if the information is
112 available to a broad audience;

113 “(iii) A telephone book or online directory;

114 “(iv) A television, Internet, or radio program; and

115 “(v) News media;

116 “(C) Observable from a publicly accessible location; or

117 “(D) That a person reasonably believes is made available lawfully to the general
118 public if:

119 “(i) The information is of a type generally available to the public; and

120 “(ii) The person has no reason to believe that a data subject with authority
121 to remove the information from public availability has directed the information to be removed.

122 “(18) “Record” means information:

123 “(A) Inscribed on a tangible medium; or

124 “(B) Stored in an electronic or other medium and retrievable in perceivable form.

125 “(19) “Sensitive data” means personal data that reveals:

126 “(A) Racial or ethnic origin, religious belief, gender, sexual orientation,
127 citizenship, or immigration status;

128 “(B) Credentials sufficient to access an account remotely;

129 “(C) A credit or debit card number or financial account number;

130 “(D) A Social Security number, tax-identification number, driver’s license
131 number, military identification number, or identifying number on a government-issued
132 identification;

133 “(E) Geolocation in real time;
134 “(F) A criminal record;
135 “(G) Income;
136 “(H) Diagnosis or treatment for a disease or health condition;
137 “(I) Genetic sequencing information; or
138 “(J) Information about a data subject the controller knows or has reason to know
139 is under 13 years of age.

140 “(20) “Sign” means, with present intent to authenticate or adopt a record:

141 “(A) Execute or adopt a tangible symbol; or

142 “(B) Attach to or logically associate with the record an electronic symbol, sound,
143 or procedure.

144 “(21) “Stakeholder” means a person that has, or represents a person that has, a direct
145 interest in the development of a voluntary consensus standard.

146 “(22) “State” means a state of the United States, the District of Columbia, Puerto Rico,
147 the United States Virgin Islands, or any other territory or possession subject to the jurisdiction of
148 the United States. The term includes a federally recognized Indian tribe.

149 “(23) “Third-party controller” means a controller that receives from another controller
150 authorized access to personal data or pseudonymized data and determines the purpose and means
151 of additional processing.

152 “§ 28-5503. Scope.

153 “(a) Except as provided in subsections (b) and (c) of this section, this chapter applies to
154 the activities of a controller or processor that conducts business in the District or produces
155 products or provides services purposefully directed to residents of the District and:

156 “(1) At any time during a calendar year maintains personal data about more than
157 50,000 data subjects who are residents of the District, excluding data subjects whose data is
158 collected or maintained solely to complete a payment transaction;

159 “(2) Earns more than 50 percent of its gross annual revenue during a calendar year
160 from maintaining personal data as a controller or processor;

161 “(3) Is a processor acting on behalf of a controller the processor knows or has
162 reason to know satisfies paragraph (1) or (2) of this subsection; or

163 “(4) Maintains personal data, unless it processes the personal data solely using
164 compatible data practices.

165 “(b) This chapter does not apply to an agency or instrumentality of the District.

166 “(c) This chapter does not apply to personal data that is:

167 “(1) Publicly available information;

168 “(2) Processed or maintained solely as part of human-subjects research conducted
169 in compliance with legal requirements for the protection of human subjects;

170 “(3) Processed or disclosed as required or permitted by a warrant, subpoena, or court
171 order or rule, or otherwise as specifically required by law;

172 “(4) Subject to a public-disclosure requirement under the Freedom of Information
173 Act, D.C. Code § 2-531 *et seq.*; or

174 “(5) Processed or maintained in the course of a data subject’s employment or
175 application for employment.

176 “§ 28-5504. Controller and processor responsibilities.

177 “(a) A controller shall:

178 “(1) If a collecting controller, provide under § 28-5505 a copy of a data subject’s
179 personal data to the data subject on request;

180 “(2) Correct or amend under § 28-5505 a data subject’s personal data on the data
181 subject’s request;

182 “(3) Provide notice under § 28-5506 about the personal data it maintains and its
183 processing practices;

184 “(4) Obtain consent under § 28-5508 for processing that is an incompatible data
185 practice;

186 “(5) Not use a prohibited data practice;

187 “(6) Conduct and maintain under § 28-5510 a data-privacy and security-risk
188 assessments; and

189 “(7) Provide redress for a prohibited data practice the controller performs or is
190 responsible for performing while processing a data subject’s personal data.

191 “(b) A processor shall:

192 “(1) On request of the controller, provide the controller with a data subject’s
193 personal data or enable the controller to access the personal data at no cost to the controller;

194 “(2) On request of the controller, correct an inaccuracy in a data subject’s
195 personal data;

196 “(3) Not process personal data for a purpose other than one requested by the
197 controller;

198 “(4) Conduct and maintain data-privacy and security-risk assessments in
199 accordance with § 28-5510; and

200 “(5) Provide redress for a prohibited data practice and the processor knowingly
201 performs in the course of processing a data subject’s personal data at the direction of the
202 controller.

203 “(c) A controller is responsible under this chapter for a prohibited data practice conducted by
204 another if:

205 “(1) The practice is conducted with respect to personal data collected by the controller;
206 and

207 “(2) The controller knew the personal data would be used for the practice and was in a
208 position to prevent it.

209 “(d) A processor is responsible under this chapter for a prohibited data practice or conducted
210 by another if:

211 “(1) The practice is conducted with respect to personal data processed by the
212 processor; and

213 “(2) The processor knew the personal data would be used for the practice and was in a
214 position to prevent it.

215 “§ 28-5505. Right to copy and correct personal data.

216 “(a) Unless personal data is pseudonymized and not maintained with sensitive data, a
217 collecting controller, with respect to personal data initially collected by the controller and
218 maintained by the controller or a third-party controller or processor, shall:

219 “(1) Establish a reasonable procedure for a data subject to request, receive a copy
220 of, and propose an amendment or correction to personal data about the data subject;

221 “(2) Establish a procedure to authenticate the identity of a data subject who
222 requests a copy of the data subject’s personal data;

223 “(3) Not later than 45 days after receiving a request from a data subject
224 authenticated under paragraph (2) of this subsection for a copy of personal data about the data
225 subject, comply with the request or provide an explanation of action being taken to comply with
226 it;

227 “(4) On request, provide the data subject one copy of the data subject’s personal
228 data free of charge once every 12 months and additional copies on payment of a fee reasonably
229 based on the collecting controller’s administrative costs;

230 “(5) Make an amendment or correction requested by a data subject if the
231 collecting controller has no reason to believe the request is inaccurate, unreasonable, or
232 excessive; and

233 “(6) Confirm to the data subject that an amendment or correction has been made
234 or explain why the amendment or correction has not been made.

235 “(b) A collecting controller shall make a reasonable effort to ensure that a correction of
236 personal data performed by the controller also is performed on personal data maintained by a
237 third-party controller or processor that directly or indirectly received the personal data from the
238 collecting controller. A third-party controller or processor shall make a reasonable effort to
239 assist the collecting controller, if necessary to satisfy a request of a data subject under this
240 section.

241 “(c) A controller may not deny a data subject a good or service, charge a different rate, or
242 provide a different level of quality to a data subject in retaliation for exercising a right under this
243 section. It is not retaliation under this subsection for a controller to make a data subject
244 ineligible to participate in a program if:

245 “(1) Corrected information requested by the data subject makes the data subject
246 ineligible for the program; and

247 “(2) The program’s terms of service specify the eligibility requirements for all
248 participants.

249 “(d) An agreement that waives or limits a right or duty under this section is
250 unenforceable.

251 “§ 28-5506. Privacy policy.

252 “(a) A controller shall adopt and comply with a reasonably clear and accessible privacy
253 policy that discloses:

254 “(1) Categories of personal data maintained by or on behalf of the controller;

255 “(2) Categories of personal data the controller provides to a processor or another
256 controller and the purpose of providing the personal data;

257 “(3) Compatible data practices applied routinely to personal data by the controller
258 or by an authorized processor;

259 “(4) Incompatible data practices that, if the data subject consents under § 28-5508,
260 will be applied by the controller or an authorized processor;

261 “(5) The procedure for a data subject to request a copy of, or propose an
262 amendment or correction to, personal data under § 28-5505;

263 “(6) Federal, state, or international privacy laws or frameworks with which the
264 controller complies; and

265 “(7) Any voluntary consensus standard adopted by the controller.

266 “(b) The privacy policy under subsection (a) of this section must be reasonably available
267 to a data subject at the time personal data is collected about the data subject.

268 “(c) If a controller maintains a public website, the controller shall publish the privacy
269 policy on the website.

270 “§ 28-5507. Compatible data practice.

271 “(a) A controller or processor may engage in a compatible data practice without the data
272 subject’s consent. A controller or processor engages in a compatible data practice if the processing is
273 consistent with the ordinary expectations of data subjects or is likely to benefit data subjects
274 substantially. The following factors apply to determine whether processing is a compatible data
275 practice:

276 “(1) The data subject’s relationship with the controller;

277 “(2) The type of transaction in which the personal data was collected;

278 “(3) The type and nature of the personal data processed;

279 “(4) The risk of a negative consequence on the data subject by use or disclosure of the
280 personal data;

281 “(5) The effectiveness of safeguards against unauthorized use or disclosure of the
282 personal data; and

283 “(6) The extent to which the practice advances the economic, health, or other
284 interests of the data subject.

285 “(b) A compatible data practice includes processing that:

286 “(1) Initiates or effectuates a transaction with a data subject with the data subject’s
287 knowledge or participation;

288 “(2) Is reasonably necessary to comply with a legal obligation or regulatory oversight
289 of the controller;

290 “(3) Meets a particular and explainable managerial, personnel, administrative, or
291 operational need of the controller or processor;

292 “(4) Permits appropriate internal oversight of the controller by the controller’s or
293 processor’s agent or external oversight by a government unit;

294 “(5) Is reasonably necessary to create pseudonymized or deidentified data;

295 “(6) Permits analysis:

296 “(A) To discover insights related to public health, public policy, or other
297 matters of general public interest and does not include use of personal data to make a prediction or
298 determination about a particular data subject; or

299 “(B) For research and development of a product or service;

300 “(7) Is reasonably necessary to prevent, detect, investigate, report on, prosecute,
301 or remediate an actual or potential:

302 “(A) Fraud;

303 “(B) Unauthorized transaction or claim;

304 “(C) Security incident;

305 “(D) Malicious, deceptive, or illegal activity;

306 “(E) Legal liability of the controller or processor; or

307 “(F) Threat to national security;

308 “(8) Assists a person or government entity acting under paragraph (7) of this
309 subsection;

310 “(9) Is reasonably necessary to comply with or defend a legal claim; or

311 “(10) Accomplishes any other purpose determined to be a compatible data
312 practice under subsection (a) of this section.

313 “(c) A controller may use personal data, or disclose pseudonymized data to a third-party
314 controller, to deliver to a data subject targeted advertising and other purely expressive content.
315 A controller may not use personal data, or disclose pseudonymized data, to offer terms to a data
316 subject that are different from terms offered to data subjects generally, including terms relating
317 to price or quality. Processing personal data or pseudonymized data for differential treatment is
318 an incompatible data practice unless the processing is otherwise compatible under this section.
319 This subsection does not prevent providing different treatment to members of a program if the
320 program’s terms of service specify the eligibility requirements for all participants.

321 “(d) A controller or processor may process personal data in accordance with the rules of a
322 voluntary consensus standard under §§ 28-5512 through 28-5515 unless a court has prohibited
323 the processing or found it to be an incompatible data practice. Processing under a voluntary
324 consensus standard is permitted only if a controller adopts and commits to the standard in its
325 privacy policy.

326 “§ 28-5508. Incompatible data practice.

327 “(a) A controller or processor engages in an incompatible data practice if the processing:

328 “(1) Is not a compatible data practice under § 28-5507 or a prohibited data practice
329 under § 28-5509; or

330 “(2) Even if a compatible data practice under § 28-5507, is inconsistent with a privacy
331 policy adopted under § 28-5506.

332 “(b) A controller may use an incompatible data practice to process personal data that does not
333 include sensitive data if, at the time the personal data is collected about a data subject, the controller
334 provides the data subject:

335 “(1) Notice and information sufficient to allow the data subject to understand the
336 nature of the incompatible data processing; and

337 “(2) A reasonable opportunity to withhold consent to the practice.

338 “(c) A controller may not process a data subject’s sensitive data using an incompatible data
339 practice without the data subject’s express consent in a signed record for each practice.

340 “(d) Unless processing is a prohibited data practice, a controller may require a data subject to
341 consent to an incompatible data practice as a condition for access to the controller’s goods or services.
342 The controller may offer a reward or discount in exchange for the data subject’s consent to process the
343 data subject’s personal data.

344 “§ 28-5509. Prohibited data practice.

345 “(a) A controller may not engage in a prohibited data practice. Processing personal data is a
346 prohibited data practice if the processing is likely to:

347 “(1) Subject a data subject to specific and significant:

348 “(A) Financial, physical, or reputational harm;

349 “(B) Embarrassment, ridicule, intimidation, or harassment; or

350 “(C) Physical or other intrusion on solitude or seclusion if the intrusion would
351 be highly offensive to a reasonable person;

352 “(2) Result in misappropriation of personal data to assume another’s identity;

353 “(3) Constitute a violation of other law, including federal or state law against
354 discrimination;

355 “(4) Fail to provide reasonable data-security measures, including appropriate
356 administrative, technical, and physical safeguards to prevent unauthorized access; or

357 “(5) Process without consent under § 28-5508 personal data in a manner that is an
358 incompatible data practice.

359 “(b) Reidentifying or causing the reidentification of pseudonymized or deidentified data is a
360 prohibited data practice unless:

361 “(1) The reidentification is performed by a controller or processor that previously had
362 pseudonymized or deidentified the personal data;

363 “(2) The data subject expects the personal data to be maintained in identified form by
364 the controller performing the reidentification; or

365 “(3) The purpose of the reidentification is to assess the privacy risk of deidentified data
366 and the person performing the reidentification does not use or disclose reidentified personal data
367 except to demonstrate a privacy vulnerability to the controller or processor that created the
368 deidentified data.

369 “§ 28-5510. Data-privacy and security-risk assessment.

370 “(a) A controller or processor shall conduct and maintain in a record a data-privacy and
371 security-risk assessment. The assessment may take into account the size, scope, and type of
372 business of the controller or processor and the resources available to it. The assessment must
373 evaluate:

374 “(1) Privacy and security risks to the confidentiality and integrity of the personal
375 data being processed or maintained, the likelihood of the risks, and the impact that the risks
376 would have on the privacy and security of the personal data;

377 “(2) Efforts taken to mitigate the risks; and

378 “(3) The extent to which the data practices comply with this chapter.

379 “(b) A controller or processor shall update the data-privacy and security-risk assessment
380 if there is a change in the risk environment or in a data practice that may materially affect the
381 privacy or security of the personal data.

382 “(c) A data privacy and security risk assessment is confidential and is not subject to the
383 Freedom of Information Act, D.C. Code § 2-531 *et seq.* or discovery rules in a civil action. The
384 fact that a controller or processor conducted an assessment, the records analyzed in the
385 assessment, and the date of the assessment are not confidential under this section.

386 “§ 28-5511. Compliance with other law protecting personal data.

387 “(a) A controller or processor complies with this chapter if it complies with a comparable
388 law protecting personal data in another jurisdiction and the Attorney General determines the law
389 in the other jurisdiction is at least as protective of personal data as this chapter. The Attorney
390 General may charge a fee to a controller or processor that requests a determination of compliance with
391 a comparable law under this subsection. The fee must reflect the cost reasonably expected to be
392 incurred by the Attorney General to determine whether the comparable law is at least as protective as
393 this chapter.

394 “(b) A controller or processor complies with this chapter with respect to processing that is
395 subject to the following acts:

396 “(1) The Health Insurance Portability and Accountability Act, Pub. L. 104-191, if
397 the controller or processor is regulated by that act;

398 “(2) The Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*, or otherwise is used
399 to generate a consumer report by a consumer reporting agency as defined in § 603(f) of the Fair
400 Credit Reporting Act, 15 U.S.C. § 1681a(f), a furnisher of the information, or a person procuring
401 or using a consumer report;

402 “(3) The Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6801 et seq.;

403 “(4) The Drivers Privacy Protection Act of 1994, 18 U.S.C. § 2721 et seq.;

404 “(5) The Family Education Rights and Privacy Act of 1974, 20 U.S.C. § 1232g; or

405 “(6) The Children’s Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 et

406 seq.

407 “§ 28-5512. Compliance with voluntary consensus standard.

408 “A controller or processor complies with a requirement of this chapter if it adopts and

409 complies with a voluntary consensus standard that addresses that requirement and is recognized

410 by the Attorney General under § 28-5515.

411 “§ 28-5513. Content of voluntary consensus standard.

412 “A stakeholder may initiate the development of a voluntary consensus standard for

413 compliance with this chapter. A voluntary consensus standard may address any requirement

414 including:

415 “(1) Identification of compatible data practices for an industry;

416 “(2) The procedure and method for securing consent of a data subject for an

417 incompatible data practice;

418 “(3) A common method for responding to a request by a data subject for a copy or

419 correction of personal data, including a mechanism for authenticating the identity of the data

420 subject;

421 “(4) A format for a privacy policy that provides consistent and fair

422 communication of the policy to data subjects;

423 “(5) Practices that provide reasonable security for personal data maintained by a

424 controller or processor; and

425 “(6) Any other policy or practice that relates to compliance with this chapter.

426 “§ 28-5514. Procedure for development of voluntary consensus standard.

427 “The Attorney General may not recognize a voluntary consensus standard unless it is
428 developed through a consensus procedure that:

429 “(1) Achieves general agreement, but not necessarily unanimity, and:

430 “(A) Includes stakeholders representing a diverse range of industry, consumer,
431 and public interests;

432 “(B) Gives fair consideration to each comment by a stakeholder;

433 “(C) Responds to each good-faith objection by a stakeholder;

434 “(D) Attempts to resolve each good-faith objection by a stakeholder;

435 “(E) Provides each stakeholder an opportunity to change the stakeholder’s
436 position after reviewing comments; and

437 “(F) Informs each stakeholder of the disposition of each objection and the
438 reason for the disposition;

439 “(2) Provides stakeholders a reasonable opportunity to contribute their knowledge,
440 talents, and efforts to the development of the standard;

441 “(3) Is responsive to the concerns of all stakeholders;

442 “(4) Consistently complies with documented and publicly available policies and
443 procedures that provide adequate notice of meetings and standards development; and

444 “(5) Permits a stakeholder to file a statement of dissent.

445 “§ 28-5515. Recognition of voluntary consensus standard.

446 “(a) On filing of a request by any person, the Attorney General may recognize a voluntary
447 consensus standard if the Attorney General finds the standard:

448 “(1) Does not conflict with any requirement of §§ 28-5505 to 28-5510;
449 “(2) Is developed through a procedure that substantially complies with § 28-5514 and
450 “(3) If necessary, reasonably reconciles a requirement of this chapter with the
451 requirements of other law.

452 “(b) The Attorney General shall adopt rules under the District of Columbia Administrative
453 Procedure Act, D.C. Code § 2-501 *et seq.*, or otherwise establish a procedure for filing a request
454 under subsection (a) of this section. The rules may require:

455 “(1) That the request be in a record demonstrating the standard and procedure through
456 which it was adopted comply with this chapter;

457 “(2) The person filing the request to indicate whether the standard has been recognized
458 as appropriate in another jurisdiction and, if so, identify the authority that recognized it; and

459 “(3) The person filing the request to pay a fee, which must reflect the cost reasonably
460 expected to be incurred by the Attorney General in acting on a request.

461 “(c) The Attorney General shall determine whether to grant or deny the request and provide
462 the reason for a grant or denial. In making the determination, the shall consider the need to promote
463 predictability and uniformity among the states and give appropriate deference to a voluntary
464 consensus standard developed consistent with this chapter and recognized by a privacy-enforcement
465 agency in another state.

466 “(d) After notice and hearing, the Attorney General may withdraw recognition of a voluntary
467 consensus standard if the Attorney General finds that the standard or its implementation is not
468 consistent with this chapter.

469 “(e) A voluntary consensus standard recognized by the Attorney General is a public record
470 under the Freedom of Information Act, D.C. Code § 2-531 *et seq.*

471 “§ 28-5516. Rules and enforcement.

472 “(a) Subject to subsection (e) of this section, the enforcement authority, remedies, and
473 penalties provided by D.C. Code §§ 28-3901 to 28-3913 apply to a violation of this chapter.

474 “(b) The Attorney General may adopt rules under the District of Columbia
475 Administrative Procedure Act, D.C. Code § 2-501 *et seq.*, to implement this chapter.

476 “(c) In adopting rules under this section, the Attorney General shall consider the need to
477 promote predictability for data subjects, controllers, and processors and uniformity among the
478 states. The Attorney General may:

479 “(1) Consult with attorneys general and other agencies with authority to enforce
480 personal-data privacy in other jurisdictions that have laws substantially similar to this chapter;

481 “(2) Consider suggested or model rules or enforcement guidelines promulgated by
482 the National Association of Attorneys General or a successor organization;

483 “(3) Consider the rules and practices of attorneys general and other agencies with
484 authority to enforce personal-data privacy in other jurisdictions; and

485 “(4) Consider voluntary consensus standards developed consistent with this
486 chapter that have been recognized by other attorneys general or other agencies with authority to
487 enforce personal-data privacy.

488 “(d) In an action or proceeding to enforce this chapter by the Attorney General in which
489 the Attorney General prevails, the Attorney General may recover reasonable expenses and costs
490 incurred in investigation and prosecution of the action or proceeding.

491 “(e) A private cause of action for a violation of this chapter is not authorized by this
492 subtitle.

493 “§ 28-5517. Limits of chapter.

494 “This chapter does not create or affect a cause of action under other law of the District.

495 “§ 28-5518. Uniformity of application and construction.

496 “In applying and construing this uniform act, a court shall consider the promotion of
497 uniformity of the law among jurisdictions that enact it.

498 “§ 28-5519. Electronic Records and Signatures in Global and National Commerce Act.

499 “This chapter modifies, limits, or supersedes the Electronic Signatures in Global and
500 National Commerce Act, 15 U.S.C. § 7001 et seq., but does not modify, limit, or supersede 15
501 U.S.C. § 7001(c), or authorize electronic delivery of any of the notices described in 15 U.S.C. §
502 7003(b).”

503 Sec. 3. Fiscal impact.

504 The Council adopts the fiscal impact statement in the committee report as the fiscal
505 impact statement required by section 602(c)(3) of the Home Rule Act, approved December 24,
506 1973 (87 Stat. 813; D.C. Code §1-206.02(c)(3)).

507 Sec. 4. Effective date.

508 This act shall take effect after approval by the Mayor (or in the event of a veto by the
509 Mayor, override of the veto by the Council, a 30-day period of Congressional review as provided
510 in section 602(c)(1) of the District of Columbia Home Rule Act, approved December 24, 1973
511 (87 Stat. 813; D.C. Code § 1-206.02(c)(1), and publication in the District of Columbia Register.

Uniform Personal Data Protection Act

drafted by the

NATIONAL CONFERENCE OF COMMISSIONERS
ON UNIFORM STATE LAWS

and by it

APPROVED AND RECOMMENDED FOR ENACTMENT
IN ALL THE STATES

at its

ANNUAL CONFERENCE
MEETING IN ITS ONE-HUNDRED-AND-THIRTIETH YEAR
JULY 10–15, 2020



WITH PREFATORY NOTE AND COMMENTS

Copyright © 2021

By

NATIONAL CONFERENCE OF COMMISSIONERS
ON UNIFORM STATE LAWS

September 28, 2021

ABOUT ULC

The **Uniform Law Commission** (ULC), also known as National Conference of Commissioners on Uniform State Laws (NCCUSL), now in its 130th year, provides states with non-partisan, well-conceived and well-drafted legislation that brings clarity and stability to critical areas of state statutory law.

ULC members must be lawyers, qualified to practice law. They are practicing lawyers, judges, legislators and legislative staff and law professors, who have been appointed by state governments as well as the District of Columbia, Puerto Rico and the U.S. Virgin Islands to research, draft and promote enactment of uniform state laws in areas of state law where uniformity is desirable and practical.

- ULC strengthens the federal system by providing rules and procedures that are consistent from state to state but that also reflect the diverse experience of the states.
- ULC statutes are representative of state experience, because the organization is made up of representatives from each state, appointed by state government.
- ULC keeps state law up-to-date by addressing important and timely legal issues.
- ULC's efforts reduce the need for individuals and businesses to deal with different laws as they move and do business in different states.
- ULC's work facilitates economic development and provides a legal platform for foreign entities to deal with U.S. citizens and businesses.
- Uniform Law Commissioners donate thousands of hours of their time and legal and drafting expertise every year as a public service, and receive no salary or compensation for their work.
- ULC's deliberative and uniquely open drafting process draws on the expertise of commissioners, but also utilizes input from legal experts, and advisors and observers representing the views of other legal organizations or interests that will be subject to the proposed laws.
- ULC is a state-supported organization that represents true value for the states, providing services that most states could not otherwise afford or duplicate.

Uniform Personal Data Protection Act

The committee appointed by and representing the National Conference of Commissioners on Uniform State Laws in preparing this act consists of the following individuals:

Harvey S. Perlman	Nebraska, <i>Chair</i>
James Bopp Jr.	Indiana
Stephen Y. Chow	Massachusetts
Parrell D. Grossman	North Dakota
James C. McKay Jr.	District of Columbia
Larry Metz	Florida
James E. O'Connor	Nebraska
Robert J. Tennesen	Minnesota
Kerry Tipper	Colorado
Anthony C. Wisniewski	Maryland
Candace M. Zierdt	North Dakota
David V. Zvenyach	Wisconsin
William H. Henning	Alabama, <i>Division Chair</i>
Carl H. Lisman	Vermont, <i>President</i>

Other Participants

Jane Bambauer	Arizona, <i>Reporter</i>
Michael Aisenberg	Virginia, <i>American Bar Association Advisor</i>
Daniel R. McGlynn	New Mexico, <i>American Bar Association Section Advisor</i>
Peter Winn	U.S. Department of Justice
Steven L. Willborn	Nebraska, <i>Style Liaison</i>
Tim Schnabel	Illinois, <i>Executive Director</i>

Copies of this act may be obtained from:

Uniform Law Commission
111 N. Wabash Ave., Suite 1010
Chicago, IL 60602
(312) 450-6600
www.uniformlaws.org

Uniform Personal Data Protection Act

Table of Contents

Prefatory Note.....	1
Section 1. Title.....	4
Section 2. Definitions.....	4
Section 3. Scope.....	10
Section 4. Controller and Processor Responsibilities	11
Section 5. Right to Copy and Correct Personal Data.....	14
Section 6. Privacy Policy	16
Section 7. Compatible Data Practice	18
Section 8. Incompatible Data Practice	22
Section 9. Prohibited Data Practice	24
Section 10. Data-Privacy and Security-Risk Assessment.....	26
Section 11. Compliance with Other Law Protecting Personal Data	27
Section 12. Compliance with Voluntary Consensus Standard.....	29
Section 13. Content of Voluntary Consensus Standard	30
Section 14. Procedure for Development of Voluntary Consensus Standard	31
Section 15. Recognition of Voluntary Consensus Standard	32
Section 16. Rules and Enforcement	34
Section 17. Limits of [Act]	37
Section 18. Uniformity of Application and Construction.....	37
Section 19. Electronic Records and Signatures in Global and National Commerce Act	37
[Section 20. Severability].....	37
Section 21. Effective Date	38

Uniform Personal Data Protection Act

Prefatory Note

Participation in today's digital economy involves the aggregation and use of much more information about individuals than generally appreciated by those individuals. For a generation, Internet content has been financed in large part by targeted advertising requiring the collection of information about both knowing and unknowing participants. Lending, insurance, and Internet commerce more generally have also come to increasingly rely on the intensive use of a greater quantity of personal data. Social media platforms encourage the voluntary posting of personal information, and that data, too, is used in ways that participants do not fully anticipate or appreciate. Technologies that monitor an individual's activities, location, and conversations have become commonplace in the digital economy. This information, collected in very large data sets, allow correlations and discernment of patterns that are applied to targeting and decision-making that may or may not be procedurally sound or acceptable to our communities. In the modern data economy, personal data not only permits a transaction to take place, but the data itself becomes a business asset to be bought and sold.

Until recently, personal information privacy or autonomy in the United States was primarily concerned with protecting individuals from unreasonable governmental intrusion. State common law developed by the mid-twentieth century against "highly offensive" intrusion and misappropriation of name or likeness – rooted in response to paparazzi photographic activity and balanced with First Amendment sensibilities. However, in the late 1960s and early 1970s, American scholars and lawmakers began to develop and recognize "Fair Information Practice Principles" (FIPPs). These principles encourage data collectors to receive consent from data subjects (or at least provide notice) before data is collected or repurposed, and they encourage data collectors to recognize an individual's right to access, correct, or delete personal data. A version of these principles was implemented in federal sectoral privacy laws such as the Fair Credit Reporting Act ("FCRA"), the Health Insurance Portability and Accountability Act ("HIPAA"), and the Privacy Act (which regulates how the federal government itself collects and uses personal data).

The European Union ("EU"), with its organizational recognition of privacy as a human right, applied FIPPs to the creation and automated processing of databases of personal information regardless of sector or context in its 1995 Data Protection Directive. This directive was refined for an EU-wide General Data Protective Regulation ("GDPR"), which went into effect in 2018. The GDPR speaks in terms of "processing" of "personal data," whether "collected from" the individual ("data subject") (Art. 13) or not (Art. 14) and appears to include information made "available" publicly. Thus, it may be said that under the GDPR and EU organizational law, the data subject has some ownership interest in their personal data, however collected. The GDPR thus imposes obligations on data collectors and data processors to inform consumers of how their data will be used, to secure their consent for each collection and use, and to delete the data upon request. Together, these obligations greatly constrain the collection and use of personal data, and the free movement of data within the EU.

In the United States, by contrast, the collection and productive use of information (including personal information) implicates free speech rights and is thus protected to some degree from government regulation. The application of the First Amendment to collection of information was exemplified in *Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011), where data collected and analyzed by private companies was found to be speech and thus protected from governmental regulation unless justified by a significant governmental interest.

By 2018, discussions about omnibus privacy protection in the United States were premised on the FIPPs (including security, notification/transparency, access, correction and deletion “rights” outside tradition U.S. notions of “privacy”). In that context, the California Consumer Privacy Protection Act (“CCPA”) adopted a comprehensive personal data protection act adopting many of the approaches of the GDPR. The Virginia Consumer Data Protection Act (“VCDPA”) adopts a similar model. However, efforts in other states have faltered because of the significant compliance costs that these laws impose on businesses and, indirectly, their customers.

Online services are most efficient when data can cross state borders. A uniform approach to personal data protection is therefore valuable. However, large international companies are subject to the GDPR and have invested considerable resources in bringing their data practices into compliance. Companies doing business in California will need to comply with the extensive regulatory structure of the California statute. The cost of compliance has required that California and Virginia limit their rules to large data collectors or processors. Smaller firms are expressly exempt. Thus, consumer data protection in these U.S. states is at once burdensome for larger companies and not applicable to smaller ones.

The Uniform Personal Data Protection Act (“UPDPA”) provides a reasonable level of consumer protection without incurring the compliance and regulatory costs associated with the California and Virginia regimes. Some provisions of the Act are applicable to all data collectors and processors within the state and thus provide overall a more extensive data protection regime. The Act recognizes the need to create an omnibus privacy law to protect personal data from the excesses and abuses of an unregulated data economy by small actors as well as large. The Act shares many of the recognizable elements of the CCPA, VCDPA and GDPR. Generally following FIPPs, the UPDPA establishes rights for data subjects to access and correct personal data and obligations for controllers and processors to provide transparency, to draft privacy and security impact assessments, and to responsibly restrict the use of personal data.

However, this Act differs from the CCPA, CDPA, and the GDPR by recognizing that the economy, the general public, and consumers themselves are often well-served by allowing expected uses of data to proceed without consent, and by permitting firms to make useful innovations that will be unexpected when first implemented. The Act is unique among U.S. privacy regulations by using the concept of compatibility introduced in the Privacy Act and applied in GDPR. A controller can process personal data without consent if the processing is aligned with the ordinary expectations or direct interests of data subjects. Consent is only required for data practices that are *incompatible* with expectations or clear interests of the data subject. The act requires a data collector to be transparent as to its compatible uses and avoids

the largely wasteful process of seeking consent for processing that is already within the expectations of the consumer.

The Act does require consent for processing that is incompatible with the expectations and direct interests of consumers. For this processing, a firm must provide notice and an opportunity for the consumer to withhold consent. The Act requires explicit consent for the incompatible processing of certain sensitive pieces of data. And it prohibits certain types of processing that create a high risk of harm to consumers.

The Act distinguishes between two types of controllers—collecting controllers and third-party controllers—and establishes that collecting controllers (who typically have a direct relationship with the data subject) provide the means for data subjects to access and correct their personal data. Any request for correction would then be transmitted by the collecting controller to downstream controllers and processors. This focuses responsibility for access and correction on the entity known by the data subject and with a preexisting established relationship. It is a fair limit to the reach of FIPPs-based data subject rights.

The Act addresses the need for uniformity, both for compliance and consumer protection, in a variety of ways. Compliance with other legislative privacy regimes, such as GDPR or CCPA, and that provide similar data protection to this Act, will be deemed to be sufficient to comply with this Act. The Act also recognizes and exempts from its terms processing governed by industry-specific federal regimes.

Adapting a comprehensive data protection act that will be applied in a wide variety of different industries presents a challenge. For example, what might be a compatible use for a small retailer may not be such a use for a large on-line seller. The Act addresses this problem by incorporating a mechanism for creation of voluntary consensus standards. The development of these standards for particular industries is a well-established process at the federal level and has been adopted for the Child On-line Privacy Protection Act. It establishes a process whereby all stakeholders of an industry—not only industry members but also consumers and persons representing the public interest—negotiate a set of specific standards that reasonably interpret the requirements of the Act within a specific context. Once established and recognized by the state's Attorney General, any controller or processor can explicitly adopt and comply with the voluntary consensus standard. Moreover, there is an expectation that a voluntary consensus standard approved in one UPDPA state will be applicable in the others.

The Act incorporates the enforcement and remedial provisions of existing consumer protection acts in the various states. Enforcement of the Act is primarily a function of the state Attorney General.

Altogether, the provisions of this act provide substantial protection to data subjects while reflecting pragmatism and optimism about the data-driven economy. The Act is pragmatic by keeping compliance costs manageable and by avoiding obvious conflicts with the First Amendment. The Act is optimistic by leaving room for unexpected, beneficial innovations in the creative use of personal data. And the Act avoids high compliance and regulatory costs associated with more restrictive regimes.

Uniform Personal Data Protection Act

Section 1. Title

This [act] may be cited as the Uniform Personal Data Protection Act.

Section 2. Definitions

In this [act]:

(1) “Collecting controller” means a controller that collects personal data directly from a data subject.

(2) “Compatible data practice” means processing consistent with Section 7.

(3) “Controller” means a person that, alone or with others, determines the purpose and means of processing.

(4) “Data subject” means an individual who is identified or described by personal data.

(5) “Deidentified data” means data that is modified to remove all direct identifiers and to reasonably ensure that the record cannot be linked to an identified data subject by a person that does not have personal knowledge of or special access to the data subject’s information.

(6) “Direct identifier” means information that is commonly used to identify a data subject, including name, physical address, email address, recognizable photograph, and telephone number.

(7) “Incompatible data practice” means processing that may be performed consistent with Section 8.

(8) “Maintains”, with respect to personal data, means to retain, hold, store, or preserve personal data as a system of records used to retrieve records about individual data subjects for the purpose of individualized communication or treatment.

(9) “Person” means an individual, estate, business or nonprofit entity, or other legal entity. The term does not include a public corporation or government or governmental subdivision, agency, or instrumentality.

(10) “Personal data” means a record that identifies or describes a data subject by a direct identifier or is pseudonymized data. The term does not include deidentified data.

(11) “Processing” means performing or directing performance of an operation on personal data, including collection, transmission, use, disclosure, analysis, prediction, and modification of the personal data, whether or not by automated means. “Process” has a corresponding meaning.

(12) “Processor” means a person that processes personal data on behalf of a controller.

(13) “Prohibited data practice” means processing prohibited by Section 9.

(14) “Pseudonymized data” means personal data without a direct identifier that can be reasonably linked to a data subject’s identity or is maintained to allow individualized communication with, or treatment of, the data subject. The term includes a record without a direct identifier if the record contains an Internet protocol address, browser, software, or hardware identification code, or other data uniquely linked to a particular device. The term does not include deidentified data.

(15) “Publicly available information” means information:

(A) lawfully made available from a federal, state, or local government record;

(B) available to the general public in widely distributed media, including:

(i) a publicly accessible website;

(ii) a website or other forum with restricted access if the information is available to a broad audience;

(iii) a telephone book or online directory;

(iv) a television, Internet, or radio program; and

(v) news media;

(C) observable from a publicly accessible location; or

(D) that a person reasonably believes is made available lawfully to the general public if:

(i) the information is of a type generally available to the public;

and

(ii) the person has no reason to believe that a data subject with authority to remove the information from public availability has directed the information to be removed.

(16) “Record” means information:

(A) inscribed on a tangible medium; or

(B) stored in an electronic or other medium and retrievable in perceivable form.

(17) “Sensitive data” means personal data that reveals:

(A) racial or ethnic origin, religious belief, gender, sexual orientation, citizenship, or immigration status;

(B) credentials sufficient to access an account remotely;

(C) a credit or debit card number or financial account number;

(D) a Social Security number, tax-identification number, driver’s license

number, military identification number, or identifying number on a government-issued identification;

(E) geolocation in real time;

(F) a criminal record;

(G) income;

(H) diagnosis or treatment for a disease or health condition;

(I) genetic sequencing information; or

(J) information about a data subject the controller knows or has reason to know is under 13 years of age.

(18) “Sign” means, with present intent to authenticate or adopt a record:

(A) execute or adopt a tangible symbol; or

(B) attach to or logically associate with the record an electronic symbol, sound, or procedure.

(19) “Stakeholder” means a person that has, or represents a person that has, a direct interest in the development of a voluntary consensus standard.

(20) “State” means a state of the United States, the District of Columbia, Puerto Rico, the United States Virgin Islands, or any other territory or possession subject to the jurisdiction of the United States. The term includes a federally recognized Indian tribe.

(21) “Third-party controller” means a controller that receives from another controller authorized access to personal data or pseudonymized data and determines the purpose and means of additional processing.

Comment

The Act regulates the processing of personal data. The Act uses the terms “information,” “record,” and “personal data” as increasingly specific categories. Information would include all

potentially interpretable signs and symbols, in any form, that create knowledge about any subject. A “record” is information that is recorded in an electronic or tangible medium. Records are a subset of information. “Personal data” is the subset of records that describe an individual. The Act avoids using the term “data” on its own, as this would be coterminous with “record.” References to “data” only appear in phrases such as “personal data” or “compatible data practice” that are defined terms in this Act.

The Act recognizes the distinction between controllers and processors. A controller is the person who determines the purpose and means of data processing. There are two types of controllers. A “collecting controller” is a person who directly collects data from a data subject and thus has a relationship with the data subject. A “third party controller” is a person who obtains personal data not directly from data subjects but from another controller, generally a collecting controller. As long as the person directs the purpose and means of a data processing the person is a data controller. A processor, on the other hand, processes personal data at the direction of a controller; a processor does not determine the purpose of processing of personal data. However, if a person with access to personal data engages in processing that is not at the direction and request of a controller, that person becomes a controller rather than a processor, and is therefore subject to the obligations and constraints of a controller.

The language in (3) that requires the controller to dictate both the “purpose and means” of processing is intended to include within the term “means” the selection of the processor to perform the processing.

The definition of “maintains” is pivotal to understanding the scope of the act. It is modeled after the federal Privacy Act’s definitions of “maintains” and “system of records”. 5 U.S.C. §552a(a)(3), (a)(5). While many individuals and businesses may accumulate data related to individuals in the form of emails or personal photographs, these records are not maintained as a system for the purpose and function of making individualized assessments, decisions, or communications, and would therefore not be within the scope of the Act under Section 3.

Personal data and deidentified data are mutually exclusive categories. Deidentified data must meet the standard of risk mitigation that makes data reasonably unlikely to be reidentified. This reasonableness standard is flexible so that it can accommodate advances in technology or data availability that may make reidentification efforts easier over time. Thus, the standard can be expected to rise as the ability to reidentify anonymized datasets rises. However, this is not a strict liability standard, nor is it one intolerant to risk. If reidentification is costly and error-prone, the data can meet the standard for de-identification even if reidentification is possible.

The broad category of “personal data” includes both direct identifying data and pseudonymized data. Data with a direct identifier (like name, social security number, or address) receives the full set of data protections under the act. By contrast, controllers using pseudonymized data are released from the requirement to provide access and correction (except in the case of sensitive pseudonymized data that is maintained in a way that renders the data retrievable for individualized communications and treatment.)

The definition of a “direct identifier” is limited to information that on its own tends to

identify and relate specifically to an individual. The definition provides an illustrative list of examples, but the list is non-exhaustive so that the definition is flexible enough to cover new forms of identification that emerge in the future. A persistent unique code that is used to track or communicate with an individual without identifying them is *not* a direct identifier, even if that unique code can be converted into a direct identifier using a decryption key. Data that includes a persistent unique code (but not the decryption key) is pseudonymized data. Data that does not include direct identifiers or persistent unique IDs maintained for individualized communication and treatment will nevertheless be pseudonymized data (as opposed to deidentified data) if it presents a reasonable risk of reidentification.

Pseudonymized data is itself a large subset of personal data that encompasses two distinct data practices, as identified by each of the clauses in the first sentence of its definition. First, some firms redact or remove direct identifiers and use the rest of the data fields for aggregate analysis or research. This usage of pseudonymized data is analogous to the intended uses of deidentified data, but the data does not qualify as deidentified because it is still “reasonably linkable to a data subject’s identity.” A second common practice is to maintain data without direct identifiers but with a unique code that permits firms to use the data for “individualized communication with, or treatment of, the data subject.” Cookie IDs, browser codes, and IP addresses have historically been used for this purpose. Both types of practices fall under the umbrella term “pseudonymized data” and are covered by many of the data protections of this act. However, pseudonymized data that is not maintained for individualized communication or treatment is not subject to the rights of access and correction. Pseudonymized data that is maintained for individualized communication or treatment is only subject to the rights of access and correction if the data includes sensitive data. Both types of pseudonymized data should have a more limited set of legal restrictions and obligations in order to incentivize the good data hygiene and practice of removing direct identifiers. *See Paul Schwartz & Daniel Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 NYU L. REV. 1814 (2011).

The act exempts public records, lawfully obtained. Laws providing for the collection, retention, and use of public records may contain privacy and security requirements or limits on how the records may be accessed and used. This act does not interfere with those other provisions.

The definition of “publicly available information” includes information accessible from a public website as well as information that is available on a nonpublic portion of a website if that nonpublic portion is nevertheless available to a large, non-intimate group of individuals. For example, if an individual shares personal data about themselves in a social media post that is accessible to all connected friends, that information is publicly available and would not fall within the scope of this Act. However, personal data that is shared with a hand-selected subset of friends through a direct message or through a highly constrained post on social media would not be publicly available.

The category of “sensitive data” described in (17)(B) includes passwords for password-protected accounts, ATM pins, all codes used for two- or multi-factor authentication, and answers to security questions used for account recovery. The category described in (17)(G)

includes diagnosis or treatment related to mental health conditions.

The definition of “stakeholder” in (19) is broad and should include consumer groups and civil society organizations that represent individuals who will be affected by a voluntary consensus standard.

Section 3. Scope

(a) Except as provided in subsections (b) and (c), this [act] applies to the activities of a controller or processor that conducts business in this state or produces products or provides services purposefully directed to residents of this state and:

(1) at any time during a calendar year maintains personal data about more than [50,000] data subjects who are residents of this state, excluding data subjects whose data is collected or maintained solely to complete a payment transaction;

(2) earns more than [50] percent of its gross annual revenue during a calendar year from maintaining personal data as a controller or processor;

(3) is a processor acting on behalf of a controller the processor knows or has reason to know satisfies paragraph (1) or (2); or

(4) maintains personal data, unless it processes the personal data solely using compatible data practices.

(b) This [act] does not apply to an agency or instrumentality of this state or a political subdivision of this state.

(c) This [act] does not apply to personal data that is:

(1) publicly available information;

(2) processed or maintained solely as part of human-subjects research conducted in compliance with legal requirements for the protection of human subjects;

(3) processed or disclosed as required or permitted by a warrant, subpoena, or court

order or rule, or otherwise as specifically required by law;

(4) subject to a public-disclosure requirement under [cite to state public records act]; or

(5) processed or maintained in the course of a data subject’s employment or application for employment.

Comment

The definition of “personal data” limits that term to data describing residents of this state. This section further constrains the scope of the Act by limiting the controllers and processors obligated to comply with the act. Personal data privacy legislation can impose significant compliance costs on controllers and processors and thus most proposals contain limits similar to those in subsections (1), (2), and (3) which limit their provisions to larger controllers or processors—ones who either process data on a significant number of data subjects or earn a significant amount of their revenue from processing personal data. The threshold numbers are in brackets and each State can determine the proper level of applicability. The main goal of the act is to ensure data is secured and used in responsible ways, and the primary compliance mechanisms imposed are the obligation to publish a privacy policy and to conduct a privacy assessment in order to make their data practices transparent. Similarly, these firms must respond to consumer access and correction rights. The result of the limitations in (a) (1)-(3), however, is to put personal data at risk when collected by smaller firms. Thus, this act also applies to smaller firms, but relieves them of the compliance obligations as long as they use the personal data only for compatible purposes. Thus, a small retailer that uses personal data only to complete payment transactions, to run a loyalty program, and to engage in marketing will be exempt since each of those practices is a compatible data practice. Similarly, a law firm maintaining personal data on fewer than 50,000 clients are exempt from the requirements of this act if they use personal data only to perform legal services or to communicate with data subjects.

By moving away from data subject consent as the basis for data processing and recognizing that data collectors are entitled to process data for compatible uses, some significant compliance costs are accordingly reduced, while placing limits on incompatible or unexpected and risky uses of data, both by large and small controllers and processors.

The processing of publicly available information is excluded from the act. There are significant First Amendment implication for placing limits on the use of public information. “Publicly available information” is defined in Section 2.

Processors and controllers who do not conduct business or market products and services to this state are outside the scope of the act.

Section 4. Controller and Processor Responsibilities

(a) A controller shall:

(1) if a collecting controller, provide under Section 5 a copy of a data subject's personal data to the data subject on request;

(2) correct or amend under Section 5 a data subject's personal data on the data subject's request;

(3) provide notice under Section 6 about the personal data it maintains and its processing practices;

(4) obtain consent under Section 8 for processing that is an incompatible data practice;

(5) not use a prohibited data practice;

(6) conduct and maintain under Section 10 data-privacy and security-risk assessments; and

(7) provide redress for a prohibited data practice the controller performs or is responsible for performing while processing a data subject's personal data.

(b) A processor shall:

(1) on request of the controller, provide the controller with a data subject's personal data or enable the controller to access the personal data at no cost to the controller;

(2) on request of the controller, correct an inaccuracy in a data subject's personal data;

(3) not process personal data for a purpose other than one requested by the controller;

(4) conduct and maintain data-privacy and security-risk assessments in accordance with Section 10; and

(5) provide redress for a prohibited data practice and the processor knowingly performs in the course of processing a data subject's personal data at the direction of the controller.

(c) A controller is responsible under this [act] for a prohibited data practice conducted by another if:

(1) the practice is conducted with respect to personal data collected by the controller;

and

(2) the controller knew the personal data would be used for the practice and was in a position to prevent it.

(d) A processor is responsible under this [act] for a prohibited data practice or conducted by another if:

(1) the practice is conducted with respect to personal data processed by the processor;

and

(2) the processor knew the personal data would be used for the practice and was in a position to prevent it.

Comment

This Section clarifies the different obligations that collecting controllers, third party controllers, and data processors owe to individuals. Third party controllers, including data brokers, are firms that decide how data is processed. They are under most of the same obligations as collecting controllers. However, they are not under the obligation to respond to access or correction requests. A right of access or correction imposed on third party controllers would increase privacy and security vulnerabilities because third party controllers are not able to verify the authenticity of the request as easily as collecting controllers. However, collecting controllers must transmit credible collection requests to downstream third party controllers and data processors who have access to the personal data requiring correction.

Subsection (c) makes clear that an actor in a supply chain that violates the act can expose their business partners to liability risk if those partners had sufficient information to know what the actor was doing. Actual knowledge is required. This ensures that all actors have incentive to avoid working with irresponsible firms, to refuse to process data in a manner that is prohibited,

and to end relationships with downstream processors or third party controllers that violate the act.

This Act does not obligate controllers or processors to delete data at the request of the data subject. This is substantially different from the GDPR, the California Consumer Privacy Act, and several privacy bills recently introduced in state legislatures. There is a wide range of legitimate interests on the part of collectors that require data retention. It also appears difficult given how data is currently stored and processed to assure that any particular data subject's data is deleted. The restriction on processing for compatible uses or incompatible uses with consent should provide sufficient protection.

Section 5. Right to Copy and Correct Personal Data

(a) Unless personal data is pseudonymized and not maintained with sensitive data, a collecting controller, with respect to personal data initially collected by the controller and maintained by the controller or a third-party controller or processor, shall:

(1) establish a reasonable procedure for a data subject to request, receive a copy of, and propose an amendment or correction to personal data about the data subject;

(2) establish a procedure to authenticate the identity of a data subject who requests a copy of the data subject's personal data;

(3) [not later than 45 days] [within a reasonable time] after receiving a request from a data subject authenticated under paragraph (2) for a copy of personal data about the data subject, comply with the request or provide an explanation of action being taken to comply with it;

(4) on request, provide the data subject one copy of the data subject's personal data free of charge once every 12 months and additional copies on payment of a fee reasonably based on the collecting controller's administrative costs;

(5) make an amendment or correction requested by a data subject if the collecting controller has no reason to believe the request is inaccurate, unreasonable, or excessive; and

(6) confirm to the data subject that an amendment or correction has been made or

explain why the amendment or correction has not been made.

(b) A collecting controller shall make a reasonable effort to ensure that a correction of personal data performed by the controller also is performed on personal data maintained by a third-party controller or processor that directly or indirectly received the personal data from the collecting controller. A third-party controller or processor shall make a reasonable effort to assist the collecting controller, if necessary to satisfy a request of a data subject under this section.

(c) A controller may not deny a data subject a good or service, charge a different rate, or provide a different level of quality to a data subject in retaliation for exercising a right under this section. It is not retaliation under this subsection for a controller to make a data subject ineligible to participate in a program if:

(1) corrected information requested by the data subject makes the data subject ineligible for the program; and

(2) the program's terms of service specify the eligibility requirements for all participants.

(d) An agreement that waives or limits a right or duty under this section is unenforceable.

Comment

The requirement to provide a copy of data or to initiate a data correction applies only to collecting controllers. These are the firms that already have a relationship with the data subject such that a secure authentication process would not unduly burden their business. A collecting controller must transmit any reasonable request for data correction to third party controllers and processors and make reasonable efforts to ensure that these third parties have actually made the requested change. Any third-party controller that receives a request for correction from a collecting controller must transmit the request to any processor or other third-party controller that it has engaged so that the entire chain of custody of personal data is corrected.

A collecting controller that controls and maintains personal data from several sources, only some of which were originally collected by the collecting controller, must nevertheless provide access to and correction of all personal data that the collecting controller has associated with the data subject. Thus, if a collecting controller comingles personal data collected directly from the data subject with data that has been collected or accessed from other sources (including

public sources and from other firms who share federated data) but is linked data subject, the access and correction rights apply to the entire set of personal data.

Access and correction rights do not apply to pseudonymized data in most cases. The only time a collecting controller will have to provide access and correction to pseudonymized data is if the data contains sensitive data, *and* the collecting controller maintains the data so that it can and will be re-associated with an individual at a later date (or transmits the pseudonymized data to a third party for its use in this way.) A collecting controller that stores user credentials and profiles of its customers can avoid the access and correction obligations if it segregates its data into a key code and a pseudonymized database so that the data fields are stored with a unique code and no identifiers. The separate key will allow the controller to reidentify a user's data when necessary or relevant for their interactions with the customers. Likewise, a collecting controller that creates a dataset for its own research use (without maintaining it in a way that allows for reassociation with the data subject) will not have to provide access or correction rights even if the pseudonymized data includes sensitive information such as gender or race. A retailer that collects and transmits credit card data to the issuer of the credit card in order to facilitate a one-time credit card transactions is not maintaining this sensitive pseudonymized data.

Subpart (c) ensures that a data subject who exercises a right to access or correction is not penalized through diminished services or access for asserting their rights. This anti-discrimination provision is narrower than those appearing in statutes that also provide a right to deletion. A variety of firms follow a business model that provides services for free or at a reduced rate in exchange for their customers providing personal data. This provision does not affect such a business model. For a denial to be prohibited by this section it must be in retaliation for a data subject's exercise of a right to access or correct data. Not every change in service following a correction of data is discriminatory. For example, a loyalty or membership club that requires members to live in a certain region may make a member ineligible for benefits if the correction to the data shows an address outside the region. Similarly, a correction of data that shows a significant increase in the data subject's risk profile may justify an increase in insurance premium rates. Neither of these or similar actions would be "retaliation" under this section.

Section 6. Privacy Policy

(a) A controller shall adopt and comply with a reasonably clear and accessible privacy policy that discloses:

- (1) categories of personal data maintained by or on behalf of the controller;
- (2) categories of personal data the controller provides to a processor or another controller and the purpose of providing the personal data;
- (3) compatible data practices applied routinely to personal data by the controller or by an authorized processor;

(4) incompatible data practices that, if the data subject consents under Section 8, will be applied by the controller or an authorized processor;

(5) the procedure for a data subject to request a copy of, or propose an amendment or correction to, personal data under Section 5;

(6) federal, state, or international privacy laws or frameworks with which the controller complies; and

(7) any voluntary consensus standard adopted by the controller.

(b) The privacy policy under subsection (a) must be reasonably available to a data subject at the time personal data is collected about the data subject.

(c) If a controller maintains a public website, the controller shall publish the privacy policy on the website.

Comment

The purpose of the required privacy policy is to provide data subjects with a transparent way to determine the scope of the data processing conducted by collecting controllers. While consent to compatible data practices is not required, the privacy policy does assure that data subjects can understand what those practices are for a particular controller and may choose not to engage with that controller or its affiliates. Thus, this helps to promote an autonomy regime for individuals with high levels of privacy concern without requiring burdensome consent instruments. The privacy policy also permits consumer advocates and the Attorney General to monitor data practices and to take appropriate action.

Controllers and processors must describe all of the personal data routinely maintained about data subjects including pseudonymized data. They must also describe compatible data practices and incompatible data practices employed with consent under Section 8 that are currently in routine use. Because the privacy policy requirement applies only to “maintained” data, controllers do not have to provide disclosures related to personal data (whether directly identified or pseudonymized) that are not used as a system of records for individualized communications or treatment. For example, email systems or pseudonymized statistical data typically would not be subject to this privacy policy requirement.

Controllers and processors do not have to explicitly state compatible data practices that are not routinely used. For example, a controller may disclose personal data that provides evidence of criminal activity to a law enforcement agency without listing this practice in its privacy policy as long as this type of disclosure is unusual.

Subsection (b) requires the privacy policy to be reasonably available to the data subject at the time data is collected. This does not require providing a data subject with individual notice. Placement of the privacy policy on a public website or posting in a location that is accessible to data subjects is sufficient.

The act does not require a controller to adopt and comply with a single or comprehensive set of voluntary consensus standards. However, if the controller does adopt such a standard, that should be stated in the privacy policy.

Section 7. Compatible Data Practice

(a) A controller or processor may engage in a compatible data practice without the data subject's consent. A controller or processor engages in a compatible data practice if the processing is consistent with the ordinary expectations of data subjects or is likely to benefit data subjects substantially. The following factors apply to determine whether processing is a compatible data practice:

- (1) the data subject's relationship with the controller;
- (2) the type of transaction in which the personal data was collected;
- (3) the type and nature of the personal data processed;
- (4) the risk of a negative consequence on the data subject by use or disclosure of the personal data;
- (5) the effectiveness of safeguards against unauthorized use or disclosure of the personal data; and
- (6) the extent to which the practice advances the economic, health, or other interests of the data subject.

(b) A compatible data practice includes processing that:

- (1) initiates or effectuates a transaction with a data subject with the data subject's knowledge or participation;
- (2) is reasonably necessary to comply with a legal obligation or regulatory oversight

of the controller;

(3) meets a particular and explainable managerial, personnel, administrative, or operational need of the controller or processor;

(4) permits appropriate internal oversight of the controller by the controller's or processor's agent or external oversight by a government unit;

(5) is reasonably necessary to create pseudonymized or deidentified data;

(6) permits analysis:

(A) to discover insights related to public health, public policy, or other matters of general public interest and does not include use of personal data to make a prediction or determination about a particular data subject; or

(B) for research and development of a product or service;

(7) is reasonably necessary to prevent, detect, investigate, report on, prosecute, or remediate an actual or potential:

(A) fraud;

(B) unauthorized transaction or claim;

(C) security incident;

(D) malicious, deceptive, or illegal activity;

(E) legal liability of the controller or processor; or

(F) threat to national security;

(8) assists a person or government entity acting under paragraph (7);

(9) is reasonably necessary to comply with or defend a legal claim; or

(10) accomplishes any other purpose determined to be a compatible data practice under subsection (a).

(c) A controller may use personal data, or disclose pseudonymized data to a third-party controller, to deliver to a data subject targeted advertising and other purely expressive content. A controller may not use personal data, or disclose pseudonymized data, to offer terms to a data subject that are different from terms offered to data subjects generally, including terms relating to price or quality. Processing personal data or pseudonymized data for differential treatment is an incompatible data practice unless the processing is otherwise compatible under this section. This subsection does not prevent providing different treatment to members of a program if the program’s terms of service specify the eligibility requirements for all participants.

(d) A controller or processor may process personal data in accordance with the rules of a voluntary consensus standard under Sections 12 through 15 unless a court has prohibited the processing or found it to be an incompatible data practice. Processing under a voluntary consensus standard is permitted only if a controller adopts and commits to the standard in its privacy policy.

Comment

Compatible data practices are mutually exclusive from incompatible and prohibited data practices described in Sections 8 and 9. Although compatible practices do not require specific consent from each data subject, they nevertheless must be reflected in the publicly available privacy policy as required by Section 6.

A data practice is compatible if it is either consistent with ordinary expectations of data subjects or beneficial to the data subject. Subsection (a) provides a list of factors that can help determine whether a practice meets one or both of those qualifying conditions. Subsection (b) provides a list of nine specific practices that are per se compatible and do not require consent from the data subject followed by a tenth gap-filling category that covers any other processing that meets the more abstract definition of “compatible data practice.” The factors listed in subsection (a) inform how the scope of “compatible data practice” should be interpreted. The catch-all provision in (b)(10) allows controllers and processors to create innovative data practices that are unanticipated and do not fall into the scope of one of the conventional compatible practices to proceed without consent as long as data subjects substantially benefit from the practice. In order to find that data subjects substantially benefit from the practice, an enforcement agency should ask whether data subjects would be likely to prefer that the processing occur and would be likely to consent to the processing if it were not for the transaction costs inherent to consenting processes.

Practices that qualify as compatible under subsection (b)(10) include detecting and reporting back to data subjects that they are at some sort of risk, e.g. of fraud, disease, or criminal victimization. Another example is processing that is used to recommend other purchases that are complements or even requirements for a product that the data subject has already placed in a virtual shopping cart. Both of these examples are now routine practices that consumers favor, but when they first emerged, seemed inappropriate. Subsection (b)(10) is intentionally reserving space, free from regulatory burdens, for win-win practices of this sort to emerge. This allowance for beneficial repurposing of data makes this act different in substance from the GDPR, which restricts data repurposing unless the controller gives data subjects a right to object to any processing outside certain limited “legitimate grounds” of the controller. (Articles 5(1)(b), 18, and 22 of the General Data Protection Regulation.)

An example of compatible data practices that fall under Subsection (b)(10):

Environmental, health, and safety innovations. A manufacturer creates a bicycle or a vehicle with a beacon that can be recognized by modern cars so that a warning sound is produced or, in the case of autonomous vehicles, so that brakes are applied to help avoid an accident. A power company uses pseudonymized energy data to optimize where and when energy is stored throughout the city. Even before these practices become commonplace, they will be compatible data practices because they confer clear benefits on the data subject.

“Generalized research” as described in (b)(6) means the use of personal data to discover insights about a population rather than an individual. This would include the use of personal data to initially train an AI or machine learning algorithm. However, subsequent use of such an AI or machine learning algorithm in order to make a prediction or decision about a data subject is not generalized research, and thus it must comply with this act through another provision. When the results of generalized research or a machine learning training process are used to create personalized communications based on a data subject’s personal data, subsection (c) will often be relevant to the determination of compatibility.

Subsection (b)(6) also recognizes routine research and development (R&D) as a compatible use. If personal data is used to develop or improve a product or service that the data subject should expect, for example to test whether a new machine learning algorithm improves the functioning of an email system, a game, or a payment system that the data subject intends to use, this processing is compatible under the research and development provision of subsection (b) (6).

Subsection (c) makes clear that the act will not require pop-up windows or other forms of consent before using data for tailored advertising. This leaves many common web practices in place, allowing websites and other content-producers to command higher prices from advertisers based on behavioral advertising rather than using the context of the website alone. This marks a substantial departure from the California Consumer Privacy Act and other privacy acts that have been introduced in state legislatures, including the Washington Privacy Act Sec. 103(5) and the proposed amendments to the Virginia Consumer Data Protection Act Sec. 59.1-573(5). All of these bills permit data subjects to opt out of the sale or disclosure of personal data for the purpose of targeted advertising.

Under subsection (c), websites and other controllers cannot use or share data even in

pseudonymized form for tailored treatment unless tailoring treatment is compatible for an entirely different reason. For example, a firm that shares pseudonymized data with a third party controller for the purpose of creating “retention models” or “sucker lists” that will be used by the third party or by the firm itself to modify contract terms cannot rely on subsection (c), because the processing is used for targeted decisional treatment. The firm also cannot rely on subsection (b)(10) or any other provision of this section because the processing is unanticipated and does not substantially benefit the data subject. (See Maddy Varner & Aaron Sankin, *Sucker List: How Allstate’s Secret Auto Insurance Algorithm Squeezes Big Spenders*, THE MARKUP (February 25, 2020) for an allegation that provides an example of this sort of processing.) By contrast, a firm that runs a wellness-related app and shares pseudonymized data with a third party controller for the purpose of researching public health generally or for assessing a health risk to the data subject specifically would be in a different posture. Like the “sucker list” example, this controller might not be able to rely on subsection (c) because the processing may be used to guide a public health intervention or to modify recommendations that the wellness app gives to the data subject. Nevertheless, the app producer could rely on subsection (b)(10) for processing that changes the function of the app itself because this processing, while potentially unanticipated, redounds to the benefit of the data subject without meaningfully increasing risk of harm. The app producer could rely on subsection (b)(6) for disclosure of pseudonymized data to produce generalized research (which then may be used for general public health interventions.)

Subsection (c) also clarifies that loyalty programs that use personal data to offer discounts or rewards are compatible practices. Although the targeted offering of discounts or rewards would constitute decisional treatment, these are accepted and commonly preferred practices among consumers. Indeed, most loyalty programs, including programs offering special rewards, premium features, discounts, or club-card privileges, would qualify as compatible practices under subsection (b)(1) since customers typically affirmatively subscribe or sign up for them in order to receive discounts and rewards.

Subsection (d) incorporates any data practice that has been recognized as compatible through a voluntary consent process as one of the per se compatible data practices, effectively adding these to the list contained in subsection (b).

Compatible data practices may be conducted without consent even if the practice is applied to sensitive personal data. For example, a company can store a client’s or customer’s credit card number for the purposes of processing future transactions. This is a common compatible use of data even though it includes “sensitive data.” As long as the controller uses reasonable data security measures, this practice does not require consent.

Section 8. Incompatible Data Practice

(a) A controller or processor engages in an incompatible data practice if the processing:

(1) is not a compatible data practice under Section 7 or a prohibited data practice under Section 9; or

(2) even if a compatible data practice under Section 7, is inconsistent with a privacy policy adopted under Section 6.

(b) A controller may use an incompatible data practice to process personal data that does not include sensitive data if, at the time the personal data is collected about a data subject, the controller provides the data subject:

(1) notice and information sufficient to allow the data subject to understand the nature of the incompatible data processing; and

(2) a reasonable opportunity to withhold consent to the practice.

(c) A controller may not process a data subject's sensitive data using an incompatible data practice without the data subject's express consent in a signed record for each practice.

(d) Unless processing is a prohibited data practice, a controller may require a data subject to consent to an incompatible data practice as a condition for access to the controller's goods or services. The controller may offer a reward or discount in exchange for the data subject's consent to process the data subject's personal data.

Comment

An incompatible data practice is a practice that can be used with consent. These practices involve an unanticipated use of data that is likely to cause neither substantial harm nor substantial benefit to the data subject. (The former would be a prohibited data practice and the latter would be a compatible one.) An example of an incompatible data practice is a firm that develops an app that sells user data to third party fintech firms for the purpose of creating novel credit scores or employability scores. Another example is a data practice that a firm routinely employs and failed to disclose in their privacy policy as required under section 6. An undisclosed practice creates a risk of consumer deception, even if the practice is a compatible data practice.

Examples of incompatible data practices include the following:

Selling or sharing data for unrestricted purposes. Providing personal data to a third-party controller for unlimited and unrestricted use is an incompatible data practice requiring consent. Moreover, if the controller knows that the third-party recipient will use the personal data for a prohibited practice, the controller providing the data will be held responsible for the prohibited act as well under Section 4(c).

Public mobility data for health risks. Using pseudonymized personal data such as location data for COVID risk assessment is a compatible data practice because it is generalized research. (Section 7(b)(6).) Using data for targeting COVID exposure risk assessments and notifications is a form of tailored communication and is likely to benefit the data user. (Section 7(c) or 7(a).) However, if a company uses personal data such as location data or COVID risk to deny entry to a building or to increase the price of a service, that use of data would be incompatible and would require consent.

Selling personal data in identified form for marketing purposes. Selling data in identified form for marketing purposes is an incompatible data practice in most cases, unless the context of data collection is such that the sale for marketing purposes falls within the reasonable expectations of the consumer.

The type of consent procedure that a controller must use depends on whether the personal data includes sensitive data. Incompatible data practices conducted on personal data that includes sensitive data requires opt-in consent, while incompatible data practices conducted on personal data that does not include sensitive data can proceed as long as the controller has provided notice and a reasonable opportunity to opt out.

Subpart (d) makes clear that a firm may condition services on consent to processing that would otherwise be incompatible. In other words, if the business model for a free game app is to sell data to third party fintech firms, the app developers will have to receive consent that meets the requirements of subpart (d). But the firm can also refuse service to a potential customer who does not consent. This is distinguishable from the California Privacy Rights Act’s nondiscrimination provision, which permits variance in price or quality of service only if the difference is “reasonably related to the value provided to the business by the consumer’s data.” (California Privacy Rights Act Section 11.)

Section 9. Prohibited Data Practice

(a) A controller may not engage in a prohibited data practice. Processing personal data is a prohibited data practice if the processing is likely to:

(1) subject a data subject to specific and significant:

(A) financial, physical, or reputational harm;

(B) embarrassment, ridicule, intimidation, or harassment; or

(C) physical or other intrusion on solitude or seclusion if the intrusion would

be highly offensive to a reasonable person;

(2) result in misappropriation of personal data to assume another’s identity;

(3) constitute a violation of other law, including federal or state law against

discrimination;

(4) fail to provide reasonable data-security measures, including appropriate administrative, technical, and physical safeguards to prevent unauthorized access; or

(5) process without consent under Section 8 personal data in a manner that is an incompatible data practice.

(b) Reidentifying or causing the reidentification of pseudonymized or deidentified data is a prohibited data practice unless:

(1) the reidentification is performed by a controller or processor that previously had pseudonymized or deidentified the personal data;

(2) the data subject expects the personal data to be maintained in identified form by the controller performing the reidentification; or

(3) the purpose of the reidentification is to assess the privacy risk of deidentified data and the person performing the reidentification does not use or disclose reidentified personal data except to demonstrate a privacy vulnerability to the controller or processor that created the deidentified data.

Comment

Subsection 9(a) prohibiting certain practices applies to controllers. Under the act, it is controllers who determine the nature of processing activities.

Reidentification of previously deidentified data is a prohibited practice unless the reidentification fits one of the exceptions in subsection (b). Exception (b)(1) covers controllers or processors that are in the practice of pseudonymizing personal data for security reasons and then reidentify the data only when necessary. This exception applies to controllers or processors who already have the right and privilege to process personal data. Exception (b)(2) covers controllers who collect pseudonymized data from other controllers with the expectation that the data will be linked to the data subject's identity and maintained in identified form. An example is a credit card issuer that receives transaction data from a retailer in pseudonymized form (with card number, for example) and subsequently associates it with a specific individual's credit account for billing and other purposes. Exception (b)(3) exempts "white hat" researchers who perform reidentification attacks in order to stress-test the deidentification protocols. These researchers may disclose the details (without

identities) of their demonstration attacks to the general public, and can also disclose the reidentifications (with identities) to the controller or processor.

Section 10. Data-Privacy and Security-Risk Assessment

(a) A controller or processor shall conduct and maintain in a record a data-privacy and security-risk assessment. The assessment may take into account the size, scope, and type of business of the controller or processor and the resources available to it. The assessment must evaluate:

(1) privacy and security risks to the confidentiality and integrity of the personal data being processed or maintained, the likelihood of the risks, and the impact that the risks would have on the privacy and security of the personal data;

(2) efforts taken to mitigate the risks; and

(3) the extent to which the data practices comply with this [act].

(b) A controller or processor shall update the data-privacy and security-risk assessment if there is a change in the risk environment or in a data practice that may materially affect the privacy or security of the personal data.

(c) A data privacy and security risk assessment is confidential and is not subject to [cite to state public records act and discovery rules in a civil action]. The fact that a controller or processor conducted an assessment, the records analyzed in the assessment, and the date of the assessment are not confidential under this section.

***Legislative Note:** The state should include appropriate language in subsection (c) exempting a data-privacy and security-risk assessment from an open records request and discovery in a civil case to the maximum extent possible under state law.*

Comment

The goal of Section 10 is to ensure that all controllers and processors go through a reflective process of evaluation that is appropriate for their size and the intensity of data use. Other than being a record, the act does not require any particular format for the evaluation. There

are many existing forms that companies can use to help them through a privacy impact assessment, and the Attorney General may recommend or provide some of these on their website.

A controller or processor must reassess the privacy and security practices of the firm when they make significant changes to their own data practices or when there is a significant change in the environment, such as an increase in the probability of a data security breach.

Under this section, the privacy and risk assessment is a confidential document and should not be subject to disclosure or discovery. The purpose is to assure the assessment is an honest assessment rather than a document produced for possible future litigation. However, the fact that an assessment was completed needs to be available to enforce the subsection. The assessment may also not be used to shield the underlying records analyzed in the assessment from disclosure. These records, however, may be protected from disclosure under other law.

Section 11. Compliance with Other Law Protecting Personal Data

(a) A controller or processor complies with this [act] if it complies with a comparable law protecting personal data in another jurisdiction and the [Attorney General] determines the law in the other jurisdiction is at least as protective of personal data as this [act]. The [Attorney General] may charge a fee to a controller or processor that requests a determination of compliance with a comparable law under this subsection. The fee must reflect the cost reasonably expected to be incurred by the [Attorney General] to determine whether the comparable law is at least as protective as this [act].

(b) A controller or processor complies with this [act] with respect to processing that is subject to the following acts [as amended]:

(1) the Health Insurance Portability and Accountability Act, Pub. L. 104-191, if the controller or processor is regulated by that act;

(2) the Fair Credit Reporting Act, 15 U.S.C. Section 1681 et seq., or otherwise is used to generate a consumer report by a consumer reporting agency as defined in Section 603(f) of the Fair Credit Reporting Act, 15 U.S.C. Section 1681a(f), a furnisher of the information, or a person procuring or using a consumer report;

- (3) the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. Section 6801 et seq.;
- (4) the Drivers Privacy Protection Act of 1994, 18 U.S.C. Section 2721 et seq.;
- (5) the Family Education Rights and Privacy Act of 1974, 20 U.S.C. Section

1232g; or

- (6) the Children’s Online Privacy Protection Act of 1998, 15 U.S.C. Section 6501

et seq.

Legislative Note: *It is the intent of this act to incorporate future amendments to the cited federal laws. In a state in which the constitution or other law does not permit incorporation of future amendments when a federal statute is incorporated into state law, the phrase “as amended” should be omitted in subsection (b) and Section 19 . The phrase also should be omitted in a state in which, in the absence of a legislative declaration, future amendments are incorporated into state law.*

Comment

Companies that collect or process personal data, particularly larger ones, have an interest in adopting a single set of data practices that satisfy the data privacy requirements of multiple jurisdictions. It is likely that such firms will adopt practices to meet the most demanding laws among the jurisdictions in which they do business. Compliance costs can be burdensome and detrimental to smaller firms that in the ordinary course of business must collect consumer data. The purpose of this section is to permit, in practice, firms to settle on a single set of practices relative to their particular data environment.

This section also greatly expands the potential enforcement resources for protecting consumer data privacy. Adoption of this act confers on the state attorney general, or other privacy data enforcement agency, authority not only to enforce the provisions of this act but also to enforce the provisions of any other privacy regime that a company asserts under subsection (a) as a substitute for compliance with this act.

The Attorney General is authorized to charge a reasonable fee for determining whether a particular law is equally or more protective than this act. It is assumed here that a reasonable consensus will be achieved within the enforcement community that will accept major comprehensive legislation as in compliance with this section. Accordingly, accepting the consensus would not require intensive activity by the Attorney General and would thus not result in a significant fee. Moreover, once another law was determined to be in compliance in a particular jurisdiction, it may not require extensive reexamination in other jurisdictions.

Subsection (b) provides exemptions for processing subject to specific federal privacy regimes. Data practices that are not subject to federal regulations under the stated enactments are governed by this act. A firm that maintains personal data solely for processing covered by the

scope of federal privacy laws identified in subsection (b) are deemed compliant with this entire Act. For example, a financial institution or medical facility that collects personal data and processes it for the purposes of delivery or billing related to financial or medical services is exempt from the obligations of the Act. But if the same firm processes personal data for the purpose of behavioral advertising, all of the notice, access, correction, and processing obligations of this Act will apply with respect to that processing.

Section 12. Compliance with Voluntary Consensus Standard

A controller or processor complies with a requirement of this [act] if it adopts and complies with a voluntary consensus standard that addresses that requirement and is recognized by the [Attorney General] under Section 15.

Comment

Developing detailed common rules for data practices applicable to a wide variety of industries is particularly challenging. Data practices differ significantly from industry to industry. This is reflected in a number of specific federal enactments governing particular types of data (HIPPA for health information) or particular industries (Graham-Leach-Bliley for financial institutions). The Act imposes fundamental obligations on controllers and data processors to protect the privacy of data subjects. These include the obligations to allow data subjects to access and copy their data, to correct inaccurate data, to be informed of the nature and use of their data, to expect their data will only be used as indicated when it is collected, and to be assured there are certain data practices that are prohibited altogether. No voluntary consensus standard may undermine these fundamental obligations.

On the other hand, how these obligations are implemented may depend on the particular business sector. Developing procedures for access, copying, and correction of personal data can be a complex undertaking for large controllers. And consumers have vastly different expectations about the use of their personal information depending on the underlying transaction for which their data is sought. Signing up for a loyalty program is far different than taking out a mortgage. Providing an opportunity for industry sectors, in collaboration with stakeholders including data subjects, to agree on methods of implementing privacy obligations provides the flexibility any privacy legislation will require. There is some experience, primarily at the federal level, of permitting industries to engage in a process to develop voluntary consensus standards that can be compliant with universal regulation and yet tailored to the particular industry.

An industry may adopt a comprehensive set of voluntary consensus standards to govern their privacy compliance policies or it may adopt a more specific standard that responds to one or more compliance requirement. For example, stakeholders of a particular industry may agree on the practices to be deemed “compatible practices” under this act, but leave other requirements to individual entity decision-making.

Voluntary consensus standards are NOT to be confused with industry codes or other

forms of self-regulation. Rather these standards must be written through a private process that assures that all stakeholders participate in the development of the standards. That process is set out in the following sections. Any concerns regarding self-regulation are also addressed in this act by requiring the Attorney General to formally recognize standards as being in substantial compliance with this Act. Thus there must be assurance that any voluntary consensus standard fully implements the fundamental privacy protections adopted by the act.

The act creates a safe harbor for covered entities that comply with voluntary consensus standards, recognized by the state Attorney General, that implements the Act's personal data privacy protections and information system security requirements for defined sectors and in specific contexts. These voluntary consensus standards are to be developed in partnership with consumers, businesses, and other stakeholders by organizations such as the American National Standards Institute, and by using a consensus process that is transparent, accountable and inclusive and that complies with due process. This safe harbor for voluntary consensus standards is modeled on Articles 40 and 41 of the GDPR, which provides for recognition of industry "codes of conduct," the Consumer Product Safety Act ("CPSA"), 15 U.S.C. § 2056, *et seq.*, which uses voluntary consensus standards to keep consumer products safe, and the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § § 6501-6506, which uses such standards to protect children's privacy online. This provision of the Act is in conformity with the Office of Management and Budget (OMB) Circular A-119, which establishes policies on federal use and development of voluntary consensus standards. Thus there is not only precedent for the adoption of voluntary consensus standards but actual experience in doing so.

By recognizing voluntary consensus standards, the Act provides a mechanism to tailor the Act's requirements for defined sectors and in specific contexts, enhancing the effectiveness of the Act's privacy protections and information system security requirements, reducing the costs of compliance for those sectors and in those contexts, and, by requiring that the voluntary consensus standard be developed through the consensus process of a voluntary consensus standards body, the concerns and interests of all interested stakeholders are considered and reconciled, thus ensuring broad-based acceptance of the resulting standard. Finally, by recognition of voluntary consensus standards by the Attorney General, the Act ensures that the voluntary consensus standard substantially complies with the Act.

Voluntary consensus standards also provides a mechanism to provide interoperability between the act and other existing data privacy regimes. The Act encourages that such standards work to reasonably reconcile any requirements among competing legislation, either general privacy laws or specific industry regulations. For example, it would provide an opportunity for firms that process both financial, health, and other data to attempt to create a common set of practices that reconcile HIPPA and GLB regulations with that applicable under this act for other personal data.

Section 13. Content of Voluntary Consensus Standard

A stakeholder may initiate the development of a voluntary consensus standard for compliance with this [act]. A voluntary consensus standard may address any requirement

including:

- (1) identification of compatible data practices for an industry;
- (2) the procedure and method for securing consent of a data subject for an incompatible data practice;
- (3) a common method for responding to a request by a data subject for a copy or correction of personal data, including a mechanism for authenticating the identity of the data subject;
- (4) a format for a privacy policy that provides consistent and fair communication of the policy to data subjects;
- (5) practices that provide reasonable security for personal data maintained by a controller or processor; and
- (6) any other policy or practice that relates to compliance with this [act].

Comment

This section clarifies the policies and practices that seem most appropriate for voluntary consensus standards and most likely to differ among industry sectors. The list of policies and practices is not intended to be exclusive. The section, however, does make clear that any such standards must remain consistent with the act's privacy protection obligations on controllers and processors.

Section 14. Procedure for Development of Voluntary Consensus Standard

The [Attorney General] may not recognize a voluntary consensus standard unless it is developed through a consensus procedure that:

- (1) achieves general agreement, but not necessarily unanimity, and:
 - (A) includes stakeholders representing a diverse range of industry, consumer, and public interests;
 - (B) gives fair consideration to each comment by a stakeholder;

(C) responds to each good-faith objection by a stakeholder;

(D) attempts to resolve each good-faith objection by a stakeholder;

(E) provides each stakeholder an opportunity to change the stakeholder's position after reviewing comments; and

(F) informs each stakeholder of the disposition of each objection and the reason for the disposition;

(2) provides stakeholders a reasonable opportunity to contribute their knowledge, talents, and efforts to the development of the standard;

(3) is responsive to the concerns of all stakeholders;

(4) consistently complies with documented and publicly available policies and procedures that provide adequate notice of meetings and standards development; and

(5) permits a stakeholder to file a statement of dissent.

Comment

This section outlines the process required for the adoption of voluntary consensus standards in order to allow them to be considered a safe harbor under this act. The process is consistent with OMB A-119 and has been utilized by industries and accepted by federal regulatory agencies. The development and operation of the process required by this section is the responsibility of the voluntary consensus organization that facilitates development of the standards. The role of the Attorney General would be only to assure that the resulting standards were developed by such a process.

Section 15. Recognition of Voluntary Consensus Standard

(a) On filing of a request by any person, the [Attorney General] may recognize a voluntary consensus standard if the [Attorney General] finds the standard:

(1) does not conflict with any requirement of Sections 5 through 10;

(2) is developed through a procedure that substantially complies with Section 14; and

(3) if necessary, reasonably reconciles a requirement of this [act] with the

requirements of other law.

(b) The [Attorney General] shall adopt rules under [cite to state administrative procedure act] or otherwise establish a procedure for filing a request under subsection (a). The rules may require:

(1) that the request be in a record demonstrating the standard and procedure through which it was adopted comply with this [act];

(2) the person filing the request to indicate whether the standard has been recognized as appropriate in another jurisdiction and, if so, identify the authority that recognized it; and

(3) the person filing the request to pay a fee, which must reflect the cost reasonably expected to be incurred by the [Attorney General] in acting on a request.

(c) The [Attorney General] shall determine whether to grant or deny the request and provide the reason for a grant or denial. In making the determination, the [Attorney General] shall consider the need to promote predictability and uniformity among the states and give appropriate deference to a voluntary consensus standard developed consistent with this [act] and recognized by a privacy-enforcement agency in another state.

(d) After notice and hearing, the [Attorney General] may withdraw recognition of a voluntary consensus standard if the [Attorney General] finds that the standard or its implementation is not consistent with this [act].

(e) A voluntary consensus standard recognized by the [Attorney General] is a public record under [cite to state public records act].

Comment

This section makes clear that the basic privacy interests of consumers will be protected throughout any voluntary consensus standards process. Each state Attorney General or other data privacy enforcement agency must assure that the rights accorded to consumers under this Act with respect to their personal data are preserved. To be recognized as compliant with this act, the Attorney General must determine that the standards were adopted through a process outlined in Section 14, which will assure that all stakeholders including representatives of data subjects are involved. The

Attorney General must also confirm that the standards are consistent with the act's imposed obligations on controllers and processors. And the Attorney General must find the standards reasonably reconcile other competing data privacy regimes.

Any industry or firm seeking to establish a set of voluntary consensus standards would have the burden of convincing the Attorney General that the standards comply with this section. It is recognized that this standard setting process can be expensive and thus the incentive for particular industries to participate will be determined in part by their expectation that standards will be treated consistently from state to state. Thus, the act contains provisions that encourage the Attorney General of each state in which this act is adopted to collaborate with Attorneys General from other states.

The Attorney General is encouraged to work with other states to achieve some uniformity of application and acceptance of these standards. While the act recognizes the State's inherent right to determine the level of data privacy protection it does encourage the Attorney General to take the actions of other states into account.

Currently the National Association of Attorneys General has created a forum through which various state Attorney Generals offices share policies and enforcement actions related to consumer protection including specifically data privacy. This activity suggests it is realistic to believe that consistency across states can be achieved.

The section also authorizes the Attorney General to charge a fee commensurate with the expense of reviewing requests for recognition of voluntary consensus standards. Such a fee is appropriate to assure adequate resources for this process and as a cost of seeking a safe harbor from otherwise applicable legislation. The Attorney General may post all approved voluntary consensus standards on a public website.

Section 16. Rules and Enforcement

(a) [Subject to subsection (e), the] [The] enforcement authority, remedies, and penalties provided by the [cite to state consumer protection act] apply to a violation of this [act].

(b) The [Attorney General] may adopt rules under [cite to state administrative procedure act] to implement this [act].

(c) In adopting rules under this section, the [Attorney General] shall consider the need to promote predictability for data subjects, controllers, and processors and uniformity among the states. The [Attorney General] may:

(1) consult with Attorneys General and other agencies with authority to enforce personal-data privacy in other jurisdictions that have laws substantially similar to this [act];

(2) consider suggested or model rules or enforcement guidelines promulgated by the National Association of Attorneys General or a successor organization;

(3) consider the rules and practices of Attorneys General and other agencies with authority to enforce personal-data privacy in other jurisdictions; and

(4) consider voluntary consensus standards developed consistent with this [act], that have been recognized by other Attorneys General or other agencies with authority to enforce personal-data privacy.

[(d) In an action or proceeding to enforce this [act] by the [Attorney General] in which the [Attorney General] prevails, the [Attorney General] may recover reasonable expenses and costs incurred in investigation and prosecution of the action or proceeding.]

[(e) A private cause of action for a violation of this [act] is not authorized by this [act] or the [cite to state consumer protection act].]

Legislative Note: *Include the first bracketed language in subsection (a), only if subsection (e) is included.*

Include subsection (d) only if the state's applicable consumer protection act does not provide for the recovery of reasonable expenses and costs.

Include bracketed subsection (e) is only if the state has a consumer protection act that authorizes a private cause of action and is the state determines that a private cause of action should not be authorized.

Comment

The challenge in uniform state legislation when agencies are given the power to adopt implementing rules and regulations is to continue to assure a reasonable degree of uniform application and enforcement of the substantive provisions. This is not a unique problem here where the state Attorney General or any other personal data privacy enforcement agency will be required to implement and enforce standards that are, by their nature, flexible so they may be implemented by diverse industries. Nor is this a problem limited to data privacy protection. Every state has adopted a general consumer protection law that governs transactions of interstate businesses within the state. The enforcement provision here is modeled after these existing acts and merely provides detail and specificity related to data privacy.

What remains uniform by adopting this act is the acknowledgement of the rights of consumers to obtain access to data held about them, to correct inaccurate data, and to be informed of the uses to which their data may be put. The distinction in this act between compatible, incompatible, and prohibited uses of personal data would create a uniform approach to the use of personal data although the very concept of “compatible” use is dependent on the nature of the underlying transaction from which the data is collected. The authorization of voluntary consensus standards provides a mechanism for achieving uniformity.

In order to encourage as much uniformity as possible, the state Attorney General is encouraged by subsection (c) to attempt to harmonize rules with those in other states that have adopted this act. The Attorney General may also consider voluntary consensus standards that have been approved in other states, but, of course, there is no requirement to accept them unless they have been previously approved in this state. These provisions are derived from section 9-526 of the Uniform Commercial Code which has been successful in harmonizing the filing rules and technologies for security interests by state filing offices. While there is not a direct analogy between privacy enforcement and filing rules, section 9-526 demonstrates that legislation can successfully encourage state officials to cooperate as a substitute for federal dictates. The National Association of Attorneys General has a data privacy working group involving representatives from several states that could facilitate uniform application of these principles.

The section applies to general policies and not to the decision to bring a particular enforcement action. The latter decision is one for prosecutorial discretion. Similarly, the application of remedies or sanctions in an individual case is left to the discretion of the Attorney General, as is true for other consumer protection enforcement actions. Whether there is a violation of the Act normally does not depend on the knowledge or mental state of the actor. However, whether the actor knows or has reason to know that a particular data practice is incompatible or prohibited should influence determination of the appropriate remedy or sanction. If the actor engages in a data practice that has been determined to violate the act in a previous enforcement action or judicial decision, knowledge of wrongdoing should be presumed.

Many states have adopted some form of private remedy for violations of their existing consumer protection acts. In some states private causes of action are authorized only for violations of established rules rather than the general prohibition against unfair or deceptive acts. Others may impose procedural requirements such as requiring plaintiffs to engage with the Attorney General before bringing a suit. See, National Consumer Law Center, *Unfair and Deceptive Acts and Practices* (9th ed. 2016).

The authorization or prohibition of a private cause of action in recent data privacy proposals has been a significant point of controversy. As section 17 makes clear, this act adopts existing state law and practice with regard to enforcement remedies and actions including whether a private cause of action is appropriate. Each state may have its own tradition for particular remedial structures. Section 17 defers to how each state has resolved these issues for violation of its existing consumer protection acts. Each state is free to determine whether its existing policies should be applicable to violations of this Act.

Nothing in this act is intended to displace traditional common law or other statutory

remedies for invasions of privacy or other wrongs.

A state may adopt subsection (d) if the recovery of costs by the Attorney General is not otherwise authorized. Subsection (d) allows the Attorney General to recover the reasonable costs of investigation and prosecution of cases under this act if the Attorney General prevails. Attorney fees are not included because in most instances those are the salaries of regular office legal staff. However, the salary costs associated with a particular case would be included in the reasonable costs of investigation and prosecution. A comparable provision was adopted recently in Virginia.

Section 17. Limits of [Act]

This [act] does not create or affect a cause of action under other law of this state.

Comment

The use of personal data can be implicated in traditional causes of action for defamation, right to privacy, intentional infliction of emotional suffering, or similar actions. In some states these actions remain at common law; in others they are creatures of statutes. This section assures that those causes of action remain unaffected by this act.

Section 18. Uniformity of Application and Construction

In applying and construing this uniform act, a court shall consider the promotion of uniformity of the law among jurisdictions that enact it.

Section 19. Electronic Records and Signatures in Global and National Commerce

Act

This [act] modifies, limits, or supersedes the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. Section 7001 et seq.[, as amended], but does not modify, limit, or supersede 15 U.S.C. Section 7001(c), or authorize electronic delivery of any of the notices described in 15 U.S.C. Section 7003(b).

[Section 20. Severability

If a provision of this [act] or its application to a person or circumstance is held invalid, the invalidity does not affect another provision or application that can be given effect without the invalid provision.]

Legislative Note: *Include this section only if the state lacks a general severability statute or a decision by the highest court of this state adopting a general rule of severability.*

Section 21. Effective Date

This [act] takes effect [180 days after the date of enactment].

Legislative Note: *A state may wish to include a delayed effective date to allow time for affected agencies and industry members to prepare for implementation and compliance.*



THE UNIFORM PERSONAL DATA PROTECTION ACT (2021)

- A Summary -

The Uniform Personal Data Protection Act, promulgated by the Uniform Law Commission in 2021, applies fair information practices to the collection and use of personal data from consumers by business enterprises. The act applies broadly to any entity that collects or maintains personal data but avoids the high compliance costs for businesses and the substantial enforcement costs for states associated with regulatory regimes modeled after the California Consumer Privacy Act and the European General Data Privacy Regulation. And the act exempts small businesses unless they use personal data in a manner that a consumer would not expect. The act also avoids the First Amendment concerns that arise from privacy laws that greatly restrict information without sufficient justification. By adapting a risk-based approach to privacy regulation, the act protects all data subjects from harmful processing and also offers the flexibility for startups and established firms to innovate.

The Act has several elements that make it more practical, more flexible, and less costly than other models of state privacy legislation. Specifically, the Uniform Personal Data Protection Act does the following:

- Authorizes some data practices, called “compatible data practices”, that may be performed without consent. Data processing is a “compatible data practice” if reasonable consumers would expect it to occur, or if the consumer directly benefits from the practice.
- Prohibits data practices that may cause a substantial risk of harm to data subjects, including processing likely to cause embarrassment, harassment, or financial harm and data storage that fails to provide reasonable data security.
- Permits “incompatible data practices”—that is, processing that is neither “compatible” nor prohibited—to be performed, but only with notice and consent.
- Promotes transparency and accountability by requiring companies to post a privacy policy identifying their uses of personal data and by giving data subjects the right to access and correct their data.
- Avoids the substantial First Amendment conflict associated with the right to data deletion.
- Authorizes personal data to be used for tailored messaging (including advertising) as a compatible use. (This provision does not cover the use of personal data to make tailored decisions about the terms of an offer to, agreement with, or treatment of an individual.)

- Requires businesses to engage in a privacy and security self-assessment, and encourages honest self-reflection by shielding the content of the self-assessment from disclosure in subsequent litigation.
- Allows businesses to avoid the costs of multiple compliance protocols by recognizing compliance with similar, or more restrictive, laws from other jurisdictions as compliance with this act.
- Limits the scope of the act to companies that collect non-public data maintained in a system of records designed for individualized treatment of or communication with data subjects, thus avoiding applicability to unstructured forms of information such as email communications.
- Exempts data processing that is already regulated by major federal privacy regimes.
- Encourages the development of voluntary consensus standards by which data controllers, processors, data subjects and other interested stakeholders can engage together to develop standards tailored to the context of particular industries.
- Incorporates enforcement provisions of existing state Consumer Protection Acts that authorize state attorneys general to monitor personal data practices and to seek redress for violations of the act.
- Encourages uniformity of enforcement in the enacting states by authorizing state attorneys general directly or through the National Association of Attorneys General, to coordinate their regulatory and enforcement policies.
- Encourages states to determine for themselves whether a private right of action should be authorized for violation of the act and provides bracketed language to prohibit such rights of action.

The Act uses subtle incentives to encourage more responsible data use. Small businesses are exempt as long as they use only “compatible” data practices. Use of personal data that is pseudonymized (data with personal identifiers removed) is subject to fewer restrictions than data with personal identifiers, thus encouraging entities to convert identified data into a form that offers more privacy and security. The act also authorizes companies to use or disclose data for general research purposes and prohibits the re-identification of pseudonymized or de-identified data. Moreover, in order to avoid unintended increased risk to data subject privacy, the act requires only those controllers who have directly collected data from consumers and who are best positioned to authenticate their identity, to respond to access and correction requests. All other downstream recipients of personal data must respond to requests that are transmitted by the collecting controller.

For more information about the Uniform Personal Data Protection Act, please contact ULC Legislative Counsel Libby Snyder at (312) 450-6619 or lsnyder@uniformlaws.org.



WHY YOUR STATE SHOULD ADOPT THE UNIFORM PERSONAL DATA PROTECTION ACT (2021)

The Uniform Personal Data Protection Act, promulgated by the Uniform Law Commission in 2021, applies fair information practices to the collection and use of personal data from consumers by business enterprises. By adapting a risk-based approach to privacy regulation, the act protects all data subjects from harmful processing and also offers the flexibility for startups and established firms to innovate.

The Act has several elements that make it more practical, more flexible, and less costly than other models of state privacy legislation. Specifically, the Uniform Personal Data Protection Act does the following:

- Applies broadly to any entity that collects or maintains personal data but exempts small businesses unless they use personal data in a manner that a consumer would not expect.
- Gives consumers the right to access and correct their personal data held by others and protects them from unexpected, potentially risky uses of their data without their consent.
- Allows businesses to avoid the costs of consent if they use data exclusively in ways that are compatible with consumer expectations and best interests.
- Provides incentives for businesses to pseudonymize personal data to enhance consumer protection and directs consumer requests for access to businesses best able to authenticate their identity.
- Reduces the compliance costs for businesses and the enforcement costs on state governments required by other more regulatory models such as the European General Data Privacy Regulation and the California Data Privacy Act.
- Respects First Amendment limitations on the regulation of personal data (*Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011)).
- Promotes compatibility by recognizing compliance with existing state and federal personal data privacy regimes as compliance with this act.
- Addresses the variety of contexts and needs for different sectors by allowing data users and data subjects to negotiate voluntary consensus standards for data use.

- Uses existing enforcement mechanisms in state consumer protection laws for enforcement of this act.
- Leaves to each state the question of whether to authorize a private cause of action for violation of the act.

Altogether, the provisions of this act provide substantial protection to data subjects while reflecting pragmatism and optimism about the data-driven economy. The Act is pragmatic by keeping compliance costs manageable and by avoiding obvious conflicts with the First Amendment. The Act is optimistic by leaving room for unexpected, beneficial innovations in the creative use of personal data. And the Act avoids high compliance and regulatory costs associated with more restrictive regimes.

For more information on the Uniform Personal Data Protection Act, please contact ULC Legislative Counsel Libby Snyder at (312) 450-6619 or lsnyder@uniformlaws.org.