



# The FAIR and OPEN USE Act

A Demonstration of Accountability-Based Legislation  
To Assure the Fair Processing of Data Pertaining to People

May 25, 2021



The Information Accountability Foundation (IAF) is a non-profit global information policy think tank that works with regulatory authorities, policymakers, business leaders, civil society and other key stakeholders to promote responsible processing of data and help frame privacy and data protection policy. IAF believes that frameworks based on risk assessment and effective information governance will enable beneficial, data-driven innovation while protecting individuals and society from the myriad potential harms that may arise from data processing in the information age.

As part of these efforts, IAF drafted the FAIR and OPEN USE Act (Model Legislation) to demonstrate how accountability-based legislation can incentivize organizations to optimize beneficial uses of data while simultaneously minimizing adverse consequences for individuals and society as a whole. While the Model Legislation is intended to be educational, the IAF also hopes that it will inform the legislative process.

The IAF developed three principles to guide the drafting of the Model Legislation.

#### Accountable and Measurable

Organizations must be responsible for how data are used and be answerable to others for the means taken to be responsible. Decisions must be explainable to others based on objective measures. In sum, the Model Legislation provides organizations with flexibility to innovate but organizations are on the hook for any adverse outcomes their actions produce.

#### Informing and Empowering

Organizations have a proactive obligation to inform stakeholders about the data processed, the processes used to assess and mitigate risk, and an individual's ability to exert control and make choices. Although a risk-based framework shifts the burden from the individual to the organization to prevent adverse outcomes, individuals still participate and have some level of control.

#### Competency, Integrity and Enforcement

Organizations are evaluated by the competency they demonstrate in reaching decisions to process data, their honesty, disclosures and actions. A well-resourced and capable regulatory enforcement mechanism is necessary to help ensure trust and compliance. Organizations are responsible for outcomes, but the Model Legislation contemplates that there is a difference between systematically bad decisions and anomalies.

Sections of the Model Legislation are color coded to highlight how the three principles are reflected and implemented in the text. Additional information about the principles may be found in [Principles for Fair Processing Accountability](#).



# A BILL<sup>1</sup>

To assure an innovative and fair digital future for all Americans by preserving America’s innovation engine; protect individuals’ interests in the fair, ethical, transparent, and responsible processing of personal data and other data that may impact an individual; mitigate risks of adverse impacts from the processing of personal data; and promote the benefits of the twenty-first century information age through an agile regulatory framework that contemplates that: (1) the sensitivity and value of data is increasingly difficult to understand and predict and (2) the majority of data about individuals is collected passively and observed through machine-to-machine transactions or computationally inferred.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

## **Article I. SHORT TITLE AND TABLE OF CONTENTS**

### **Section 1.01 SHORT TITLE AND TABLE OF CONTENTS.**

(a) SHORT TITLE.—This Act may be cited as the “Fair Accountable Innovative Responsible and Open Processing Enabling New Uses that are Secure and Ethical Act” or the “FAIR and OPEN USE Act”.

(b) Table of Contents.—

(1) Article I. Short Title and Table of Contents

1) Section 1.01 Short Title and Table of Contents

2) Section 1.02 Findings and Purpose

3) Section 1.03 Definitions

(2) Article II. Fair Processing of Personal Data<sup>2</sup>

1) Section 2.01 Lawful, Responsible, and Fair Processing

2) Section 2.02 Restrictions on Processing

---

<sup>1</sup> In order to help the reader understand the draft bill, all defined terms are capitalized throughout the document. We acknowledge that this is not legislative drafting convention.

<sup>2</sup> The IAF Model does not use the word “privacy.” The term is imprecise and lacks a common definition. Even the [International Association of Privacy Professionals website](#) states, “What does privacy mean? Well, it depends on who you ask.” It’s difficult to craft a legislative solution to solve an undefined problem. In addition, traditional notions of “privacy” do not capture the full range of issues and risks presented by the processing of personal data in the information age. A future-oriented, legal framework should promote fair processing and broadly address how processing data can impact people in a highly observational digital ecosystem.

- 25 3) Section 2.03 Unethical and Reckless Processing
- 26 (3) Article III. Responsibilities of Accountable Covered Entities
- 27 1) Section 3.01 Open and Transparent Processing
- 28 2) Section 3.02 Meaningful Control
- 29 3) Section 3.03 Data Quality, Accuracy, and Retention
- 30 4) Section 3.04 Access and Data Portability
- 31 5) Section 3.05 Responsible and Accessible Redress
- 32 6) Section 3.06 Data Security
- 33 7) Section 3.07 Procedures, Exceptions, and Rule of Construction
- 34 (4) Article IV. Accountable Processing
- 35 1) Section 4.01 Accountable Processing Management Program
- 36 2) Section 4.02 Ethical, Trustworthy, and Preventative Design
- 37 3) Section 4.03 Accountability for Automated Decision Making
- 38 4) Section 4.04 Accountability for Processing by Service Providers
- 39 and Third Parties
- 40 5) Section 4.05 Workforce Accountability
- 41 6) Section 4.06 Oversight: Demonstrating Trustworthiness,
- 42 Compliance, and Ongoing Commitment to Responsible
- 43 Processing
- 44 (5) Article V. Processing Risk Management
- 45 1) Section 5.01 Risk Management Strategy
- 46 2) Section 5.02 Assessment of Processing Risk
- 47 3) Section 5.03 Categorization of Processing Risk
- 48 4) Section 5.04 Processing Impact Assessments
- 49 5) Section 5.05 Enhanced Processing Impact Assessment to Assess
- 50 Implications of Automated Decision Making
- 51 6) Section 5.06 Bad Faith
- 52 7) Section 5.07 Rulemaking
- 53 (6) Article VI. Enforcement by Commission and State Attorneys General
- 54 1) Section 6.01 Enforcement by Commission
- 55 2) Section 6.02 Enforcement by State Attorneys General

- 56 3) Section 6.03 Safe Harbor Programs for Responsible and  
57 Accountable Covered Entities  
58 4) Section 6.04 Safe Harbor for Accountable Small Business and  
59 Non-Profit Organizations  
60 5) Section 6.05 Accountability Reports and Assessments  
61 6) Section. 6.06 Implementing Regulations to Support  
62 Accountability  
63 (7) Article VII. Commission Education, Guidance, Outreach, and Reports  
64 1) Section 7.01 Consumer Education  
65 2) Section 7.02 Guidance and Outreach for Covered Entities  
66 3) Section 7.03 International Cooperation for the Protection of  
67 Personal Data  
68 4) Section 7.04 Report  
69 (8) Article VIII. Commission Resources and Authorization of  
70 Appropriations  
71 1) Section 8.01 Appointment of Additional Personnel  
72 2) Section 8.02 Authority to Establish New Bureau or Office  
73 3) Section 8.03 Authorization of Appropriations  
74 (9) Article IX. Preemption  
75 1) Section 9.01 Preemption  
76 2) Section 9.02 Effect on Other Laws  
77 3) Section 9.03 Government Accountability Office Study and Report  
78 (10) Article X. Effective Date and Savings Clause  
79 1) Section 10.01 Effective Date  
80 2) Section 10.02 No Retroactive Applicability  
81 3) Section 10.03 Savings Clause  
82

83 **Section 1.02 FINDINGS AND PURPOSE.**

- 84 (a) The United States' information ecosystem is the world's most  
85 innovative. It has not just driven economic growth; it has facilitated  
86 positive changes in all sectors.

- 87 (b) The rapid evolution of lifechanging digital products, services, and  
88 consumer applications, however, has produced equally awesome  
89 challenges for individuals and society. Today, personal data<sup>3</sup> is not only  
90 collected directly from the individual but, rather, from a diverse range  
91 of sources without the individual’s awareness of the personal data’s  
92 origination and subsequent uses. In addition, a growing proportion of  
93 human activity is captured as data and groundbreaking technologies  
94 extract value from data to create new knowledge in ways once thought  
95 impossible.
- 96 (c) These complex, twenty-first century challenges cannot adequately be  
97 addressed by relying on twentieth century notions of notice, choice, and  
98 consent. Organizations that collect, create, use, and share data that may  
99 impact an individual must be responsible stewards of that data and be  
100 held accountable when their data practices create an unreasonable risk  
101 of harm to individuals or society.
- 102 (d) The rapid growth of innovative, data-driven technologies and the  
103 processing of data raises issues with respect to intrusion into seclusion,  
104 individual autonomy, fair use of an individual’s data, the just use of that  
105 data, respect for civil rights, and individual freedom.
- 106 (e) The processing of data, including personal data, also raises issues with  
107 respect to societal interests including the protection of marginalized and  
108 vulnerable groups of individuals; the safeguarding of foundational  
109 values of the democracy of the United States, such as freedom of  
110 information, freedom of speech, justice, and human ingenuity and  
111 dignity; and the integrity of democratic institutions, including fair and  
112 open elections.

---

<sup>3</sup> Technically the terms “data” and “information” have distinct definitions. The National Institute of Standards and Technology (NIST), for example, defines “data” as “pieces of information from which ‘understandable information’ is derived” and defines “information” as the “meaningful interpretation or expression of data.” [NIST Guidelines for Media Sanitization, Publication 800-88 Rev. 1](#) In most contexts today, however, the two words are used interchangeably. Adding to the confusion, some privacy laws use the term “personal data” while others use “personal information.” The IAF Model focuses on the term “data” but uses “information” in some contexts. For the purpose of interpretation, implementation, compliance, and enforcement, the two terms do not have a meaningful distinction.



- 113 (f) Data use must be—  
114 (1) legal, the data used in a specific manner is specifically authorized or  
115 not prohibited;  
116 (2) fair, data is used in a manner that maximizes stakeholder interests and  
117 mitigates risks to the extent possible; and  
118 (3) just, inappropriate discrimination should be avoided even if the  
119 outcomes are maximized for many stakeholders.
- 120 (g) Data use should support the value of human dignity—an individual has  
121 an innate right to be valued, be respected, and receive ethical treatment.  
122 An individual should not be subject to secret processing of data that  
123 pertains to the individual or will have an impact on the individual.
- 124 (h) The benefits of the information age belong to everyone. Data should not  
125 just serve the interests of the organization that collected the data.
- 126 (i) We live in a complex, data-driven world with diverse business models  
127 and infinite possibilities for innovation. This reality requires an equally  
128 complex, nuanced, innovative, and agile policy and regulatory  
129 response.<sup>4</sup>
- 130 (j) Legal frameworks structured as a list of prohibitions are dated by the  
131 time they go into effect and may unnecessarily restrict beneficial uses  
132 of data.
- 133 (k) Legislative proposals that rely primarily on notice and consent are also  
134 ineffective. Given the complexity of the digital ecosystem and  
135 asymmetry of information, the burden of preventing harm from  
136 processing data should not fall upon the individual.
- 137 (l) In today’s data-driven economy, organizations must be responsible  
138 stewards of data and accountable for their actions. Accountable

---

<sup>4</sup> IAF recognizes the appeal of simple solutions but difficult digital challenges that evolve in real time cannot be solved with a short, simple legislative solution. There is no quick, easy, overnight fix to the myriad challenges presented by processing personal data. IAF drafted the IAF Model with 2030 in mind, rather than focus on what many believe are the greatest challenges today. IAF contemplates that full implementation and compliance with the framework codified in the IAF Model will take years for most entities. This is intended to be a long-term solution to a rapidly evolving set of challenges that will grow more complicated over time.

139 organizations identify and avoid unacceptable levels of risk and are  
140 answerable for any misuse of data. Accountability also requires  
141 organizations to have policies that link to the law, mechanisms to put  
142 those policies in place, security safeguards, internal oversight, and  
143 documentation for basic processes.

144 (m) The United States needs a new twenty-first century paradigm for  
145 regulating the use of data that incentivizes organizations to optimize  
146 beneficial uses of data while simultaneously minimizing adverse  
147 consequences for individuals and society as a whole. A national  
148 framework based on accountability and risk assessment, backed by  
149 robust oversight and enforcement, meets this objective.<sup>5</sup>

### 150 **Section 1.03 DEFINITIONS.**

151 (a) ADVERSE PROCESSING IMPACT.—<sup>6</sup>The term “Adverse Processing  
152 Impact” means detrimental, deleterious, or disadvantageous  
153 consequences to an Individual arising from the Processing of that  
154 Individual’s Personal Data or to society from the Processing of Personal  
155 Data, including—  
156 (1) direct or indirect financial loss or economic harm;  
157 (2) physical harm, harassment, or threat to an Individual or property;

---

<sup>5</sup> The first draft of the IAF Model was published in 2018. Dozens of stakeholders reviewed and commented on drafts of the IAF Model. International and state laws and regulations and proposed bills were reviewed and where appropriate were incorporated (some of these inclusions are reflected in the footnotes). IAF thanks the many individuals who provided their input. This draft of the IAF Model is significantly improved because of their contributions.

<sup>6</sup>The IAF Model does not use the terms “harm” or “injury.” Instead, the IAF Model defines a broad concept of “Adverse Processing Impact.” The definition of Adverse Processing Impact aligns with the approach to privacy risk and “privacy problems” codified in the National Institute of Standards and Technology’s publication, [NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0 2020](#) (“NIST Privacy Framework”). NIST defines privacy events as “potential problems individuals could experience arising from system, product, or service operations with data, whether in digital or non-digital form, through a complete life cycle from data collection through disposal. NIST Privacy Framework at p. 3. NIST identifies the range of problems an individual can experience as a result of processing as ranging from dignity-type effects such as embarrassment or stigmas to more tangible harms such as discrimination, economic loss, or physical harm. Id. The definition of Adverse Processing Impact is also generally consistent with NIST’s [Catalog of Problematic Data Actions and Problems](#), which is a non-exhaustive, illustrative set of problematic data actions and problems that individuals could experience as the result of data processing.

- 158 (3) psychological harm, including anxiety, embarrassment, fear, and other  
159 mental trauma;
- 160 (4) inconvenience or expenditure of time;
- 161 (5) a negative outcome or decision with respect to an Individual’s  
162 eligibility for a right, privilege, or benefit related to—
- 163 (A) employment, including hiring, firing, promotion, demotion,  
164 reassignment, or compensation;
- 165 (B) credit and insurance, including denial of an application, obtaining  
166 less favorable terms, cancellation, or an unfavorable change in terms  
167 of coverage;
- 168 (C) housing;
- 169 (D) education admissions;
- 170 (E) financial aid;
- 171 (F) professional certification;
- 172 (G) issuance of a license; or
- 173 (H) the provision of health care and related services.
- 174 (6) stigmatization or reputational injury;
- 175 (7) disruption and intrusion from unwanted commercial communications  
176 or contacts;
- 177 (8) discrimination in violation of Federal antidiscrimination laws or  
178 antidiscrimination laws of any State or political subdivision thereof;
- 179 (9) loss of autonomy<sup>7</sup> through acts or practices that are not reasonably  
180 foreseeable by an Individual and that are intended to materially—
- 181 (A) alter that Individual’s experiences;
- 182 (B) limit that Individual’s choices;
- 183 (C) influence that Individual’s responses; or

---

<sup>7</sup> The concept of “loss of autonomy” is widely recognized in many bills and frameworks including the NIST Privacy Framework, which provides that, “[l]oss of autonomy includes losing control over determinations about information processing or interactions with systems/products/services, as well as needless changes in ordinary behavior, including self-imposed restrictions on expression or civic engagement.” [Catalog of Problematic Data Actions and Problems](#).

- 184 (D) predetermine results or outcomes for that Individual; or<sup>8</sup>
- 185 (10) other detrimental or negative consequences that affect an Individual’s
- 186 private life, privacy affairs, private family matters or similar
- 187 concerns, including actions and communications within an
- 188 Individual’s home or similar physical, online, or digital location,
- 189 where an Individual has a reasonable expectation that Personal Data or
- 190 other data will not be collected, observed, or used.
- 191 (b) AFFIRMATIVE EXPRESS CONSENT.—The term “Affirmative Express
- 192 Consent” means a clear affirmative act establishing a freely given,
- 193 specific, informed, and unambiguous indication of the Individual’s
- 194 agreement to the Processing of Personal Data relating to the Individual.
- 195 (c) AUTOMATED DECISION MAKING.—The term “Automated Decision
- 196 Making” means the use of algorithms, machine learning, artificial
- 197 intelligence, predictive analytics, or other automated methods to make
- 198 or facilitate decisions affecting Individuals. Automated Decision
- 199 Making—
- 200 (1) includes techniques—
- 201 (A) performed by or in computer software, physical hardware, or any
- 202 other digital context; and
- 203 (B) designed to learn to approximate a cognitive task, solve complex
- 204 problems, make predictions, define or identify correlations, approve
- 205 or deny transactions, grant or decline permissions, adapt to changing
- 206 circumstances, or improve performance when exposed to new or
- 207 existing data sets; and
- 208 (2) may operate with varying levels of autonomy or human intervention.
- 209 (d) BENEFIT TO INDIVIDUALS AND COMPETITION.—The term “Benefit to
- 210 Individuals and Competition” means a material, objective, and
- 211 identifiable positive effect or advantageous outcome—

---

<sup>8</sup> The IAF Model applies the well accepted drafting convention that “or” means “either or both”, or if there is a series of items, “anyone item or combination of items”.

- 212 (1) to Individuals or the marketplace as a result of the Processing of  
213 Personal Data; and
- 214 (2) which is separate and distinct from any positive outcome,  
215 advantageous impact, or value that accrues to a Covered Entity, single  
216 person or Individual, or a narrow or specific group of persons.
- 217 (e) BIOMETRIC DATA.—The term “Biometric Data” means an Individual’s  
218 physiological, biological, or behavioral characteristics, including an  
219 Individual’s deoxyribonucleic acid (DNA), that can be used, alone or in  
220 combination with each other or with other Personal Data, to establish  
221 Individual identity.<sup>9</sup>
- 222 (f) COMMISSION.—The term “Commission” means the Federal Trade  
223 Commission.
- 224 (g) CONSISTENT WITH THE CONTEXT.—The term “Consistent with The  
225 Context” means Processing which is consistent with the context of the  
226 relationship between the Individual and the Covered Entity and within  
227 the reasonable expectation of similarly situated Individuals. To  
228 determine whether Processing is within the reasonable expectation of  
229 similarly situated Individuals, a Covered Entity shall consider—
- 230 (1) the source of the Personal Data and the method of collection,  
231 including whether the Personal Data was collected directly from the  
232 Individual;
- 233 (2) whether the specific use is necessary to provide the specific good or  
234 service that was affirmatively and unambiguously requested by the  
235 Individual;
- 236 (3) the extent to which an Individual engaged in one or more transactions  
237 directly with the Covered Entity, including whether—
- 238 (A) the Individual intended to interact with the Covered Entity; or

---

<sup>9</sup> Biometric data includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted as well as keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data containing identifying information. A bill could incorporate these examples as well as specific exceptions.

- 239 (B) the Individual and Covered Entity maintain an ongoing commercial  
240 or other relationship;
- 241 (4) whether the specific use of the Personal Data would be obvious to an  
242 Individual under the circumstances;
- 243 (5) with respect to Observed Data, the extent to which an Individual is  
244 likely to be aware of the observation occurring as a result of the  
245 presence of sensors or other devices, is likely to be aware that such  
246 sensors or devices are creating or Processing Observed Data about the  
247 Individual, or otherwise has knowledge of the Processing;
- 248 (6) the extent to which Processing may produce unanticipated revelations  
249 about an Individual;
- 250 (7) the extent to which the Processing involves Sensitive Personal Data;
- 251 (8) the extent to which the Processing, a Processing Activity, Processing  
252 Action, business practice, or use of technology is new, novel, or not  
253 yet widely deployed in a commercial context;
- 254 (9) the age and sophistication of similarly situated Individuals who use  
255 the Covered Entity’s products or services, including whether a product  
256 or service is directed toward or significantly used by a vulnerable  
257 population identified in Section 5.02(j) of this Act;
- 258 (10) the level of Processing Risk associated with the specific Processing  
259 Activity; and
- 260 (11) the specific Adverse Processing Impact that may arise from the  
261 Processing considered from the perspective of the Individual and  
262 taking into account the full range of potential Adverse Processing  
263 Impacts identified in Section 1.03(a) of this Act.
- 264 (h) COVERED ENTITY.—<sup>10</sup>

---

<sup>10</sup> The definition of Covered Entity is consistent with most draft privacy bills. It closes the gap in FTC jurisdiction over common carriers and non-profit organizations, as a comprehensive framework must be equally applicable to every sector of our global, digital economy. The IAF Model does not exempt small businesses from the law entirely, following the approach taken in the Brookings Institution’s proposed legislation, the [Information Privacy Act](#) – June 3, 2020. Rather, the IAF Model takes into account the unique compliance and implementation challenges small businesses may face by providing different standards and less severe penalties in certain contexts. The IAF Model is scalable to organizations of all sizes and complexities.

- 265 (1) The term “Covered Entity” means—
- 266 (A) any person subject to the authority of the Commission pursuant to
- 267 section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C.
- 268 45(a)(2));
- 269 (B) notwithstanding section 5(a)(2) of the Federal Trade Commission
- 270 Act (15 U.S.C. 45(a)(2)), a common carrier subject to the
- 271 Communications Act of 1934 (47 U.S.C. 151 et seq.); or
- 272 (C) notwithstanding sections 4 and 5(a)(2) of the Federal Trade
- 273 Commission Act (15 U.S.C. 44 and 45(a)(2)), any non-profit
- 274 organization, including any organization described in section 501(c)
- 275 of the Internal Revenue Code of 1986 that is exempt from taxation
- 276 under section 501(a) of the Internal Revenue Code of 1986;<sup>11</sup> and
- 277 (D) such person, common carrier, or non-profit organization is or has
- 278 engaged in Processing Personal Data.
- 279 (2) Such term does not include—
- 280 (A) the Federal Government or any instrumentality of the Federal
- 281 Government;<sup>12</sup>
- 282 (B) the government of any State or political subdivision of any State; or
- 283 (C) an Individual Processing Personal Data—
- 284 (i) in the context of purely personal or household activities; or
- 285 (ii) acting in a de minimis commercial capacity.
- 286 (i) IDENTIFIABLE INDIVIDUAL.—The term “Identifiable Individual” means
- 287 an Individual who can be identified, directly or indirectly, by an
- 288 identifier such as a name, an identification number, location data, an
- 289 online identifier, or one or more factors specific to the physical,

---

<sup>11</sup> As with small business, accommodations have been made to take into account the potential challenges for non-profits. Non-profits, for example, are not subject to certain provisions in the Act including civil penalties or regulatory reviews as provided for in Section 6.04 of the Act. Moreover, there is a safe harbor for certain non-profits and FTC rulemakings must consider the impact of any new regulations on both non-profits and small business.

<sup>12</sup> As with other draft Federal privacy laws, the IAF Model does not address Processing by government entities. Therefore, the IAF Model does not address head on the core privacy and surveillance concerns raised in [Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems, judgment of 16 July 2020](#) (“Schrems II”). Accountable organizations can take steps to limit government access, but commercial privacy legislation alone likely will not provide a “quick fix” to the concerns raised by the Schrems II decision.

290 physiological, genetic, mental, economic, cultural, or social identity of  
291 that Individual.

292 (j) INDIVIDUAL.—The term “Individual” means a living natural person or  
293 an agent, trustee, or representative acting on behalf of a living natural  
294 person.

295 (k) INFERRED DATA.—<sup>13</sup>The term “Inferred Data” means Personal Data  
296 created or derived through the analysis or interpretation of input data,  
297 features of data, assumptions, and generalizations that is probabilistic in  
298 nature. Uses of Inferred Data include, but are not limited to predictive  
299 purposes, classifying, categorizing, segmenting, profiling,  
300 personalization, customization, decision-making, risk or eligibility  
301 assessment, or other scoring.

302 (l) OBSERVED DATA.—The term “Observed Data” means Personal Data  
303 captured by automatically recording the actions of an Individual.  
304 Observed Data includes data collected automatically by a Covered  
305 Entity, such as—

306 (1) static or video images collected from cameras;  
307 (2) voice or other audible data collected from microphones;  
308 (3) data regarding an Individual’s real-time location, location history over  
309 time, or movements collected through global positioning systems  
310 (GPS), a device’s proximity to Wi-Fi hotspots, cell tower  
311 triangulation, or other similar automated method;  
312 (4) data about an Individual’s movements, behavior, or health collected  
313 from connected device sensors, such as a gyroscope, accelerometer,

---

<sup>13</sup> The IAF Model defines four broad categories of Personal Data based on how the data originates: Provided by the Individual; Provided by a Third-Party; Observed; and Inferred. IAF believes that to get governance and risk assessment right, a Covered Entity must understand where data comes from, how it is created, and how aware and involved the Individual is in its creation. In the IAF Model, different obligations apply to different categories of data. A detailed explanation of the different categories may be found in IAF’s paper, “[The Origins of Personal Data and its Implications for Governance](#).” Many other proposed bills draw similar distinctions between different categories of data based on the source of the data.



314 magnetometer, proximity sensor, ambient light sensor, touchscreen  
315 sensor, pedometer, barometer, heart rate sensor, or thermometer; and  
316 (5) data about an Individual’s browser history, mobile application use,  
317 online posts, comments or similar digital communications, social  
318 media use, or interactions with similar devices, platforms, or  
319 applications.

320 (m) PERSONAL DATA.—

321 (1) The term “Personal Data” means information that identifies, relates to,  
322 describes, is reasonably capable of being associated with, could  
323 reasonably be linked, directly or indirectly, with a particular  
324 Individual.

325 (2) Such term does not include information about employees or  
326 employment status collected or used by an employer pursuant to an  
327 employer-employee relationship.<sup>14</sup>

328 (n) PRECISE GEOLOCATION DATA.—The term “Precise Geolocation Data”  
329 means data obtained from a device about the physical location of that  
330 device that is sufficiently precise to locate a specific Individual or  
331 device with reasonable specificity.<sup>15</sup>

332 (o) PROCESSING.—The term “Processing” means any operation or set of  
333 operations which is performed on Personal Data, such as collection,  
334 creation, recording, structuring, storage, analysis, adaptation or  
335 alteration, retrieval, consultation, use, retention, duplication, disclosure,

---

<sup>14</sup> Unlike most other proposed frameworks today, this definition of “Personal Data” does not carve out public information or publicly available information. Rather, the extent to which data is publicly available or public is a factor to be considered in a risk assessment. This is in line with laws such as the [Privacy Act of 1974](#), 5 U.S.C. § 552a et seq., which recognizes that publicly available information, such as newspaper clippings or press releases, take on a different value when incorporated in government systems. Data, including public data, takes on a different value when maintained in the context of information about an individual rather than when maintained in a library - not in a file tied to a person. Sources and context also matter. Some “public data” may be “observed data” if it’s scraped from a website without authorization or an agreement with the operator of the website. How the personal data is used or intended to be used is relevant to the analysis. Broad exceptions for public data may make compliance easier, but the distinction is becoming increasingly irrelevant and inconsistent with the policy objectives of limiting harmful uses of data.

<sup>15</sup> Unlike some proposed definitions, this definition does not refer to a specific radius. Any radius selected would be arbitrary and will become outdated as technology quickly evolves. In the context of a risk-based framework, it is more important to understand the accuracy and intended use of the data. Ease of compliance today should not trump sound policy objectives designed to promote a robust and trustworthy data-driven marketplace for tomorrow.

336 dissemination, Transfer, deletion, disposal, or destruction. Processing  
337 includes an operation or set of operations performed on data that results  
338 in the creation of Personal Data.

339 (p) PROCESSING ACTION.—<sup>16</sup>The term “Processing Action” means a  
340 single, discrete Processing operation performed on Personal Data, often  
341 characterized as one stage of the information lifecycle, including  
342 collection, creation, recording, structuring, storage, analysis, adaptation  
343 or alteration, retrieval, consultation, use, retention, duplication,  
344 disclosure, dissemination, Transfer, deletion, disposal, or destruction.

345 (q) PROCESSING ACTIVITY.— The term “Processing Activity” means a  
346 discrete set of resources organized for Processing or a specific set of  
347 Processing Actions performed on Personal Data that define the context  
348 and circumstances under which Personal Data is Processed in order to  
349 provide a logical and consistent frame of reference for assessing  
350 Processing Risk.

351 (1) Such circumstances may include the purpose of the Processing; legal  
352 or regulatory requirements; contractual obligations; boundaries of an  
353 information technology system or platform; accountable organization  
354 within a Covered Entity; stages within the lifecycle of Personal Data;  
355 or the Individual, Covered Entity, and other stakeholders directly or  
356 indirectly served or affected by the Processing.

357 (2) A Processing Activity may be identified with reference to a specific  
358 system, product, service, technology, method of Processing, business  
359 model, business function, or other item or activity as determined by a  
360 Covered Entity pursuant to a documented policy.

361 (r) PROCESSING RISK.—<sup>17</sup>The term “Processing Risk” means the level of  
362 Adverse Processing Impact potentially created as a result of or caused

---

<sup>16</sup> The NIST Privacy Framework describes these data operations in the singular as a data action and collectively as data processing. [NIST Privacy Framework](#) at p.3.

<sup>17</sup> This tracks NIST’s definition of “privacy risk” in the NIST Privacy Framework, which is “[t]he likelihood that individuals will experience problems resulting from data processing, and the impact should they occur.” [NIST Privacy Framework](#), Appendix B: Glossary, at p. 30. This maps to the generally accepted concept of risk as a function of likelihood and severity. As defined by NIST, risk is a “measure of the extent to which an entity is

363 by Processing, a specific Processing Activity, or a specific Processing  
364 Action assessed as a function of—

365 (1) the likelihood Adverse Processing Impact will occur as a result of  
366 Processing, a specific Processing Activity, or a specific Processing  
367 Action; and

368 (2) the degree, magnitude, or potential severity of the Adverse Processing  
369 Impact should it occur.

370 (s) PROVIDED DATA.—The term “Provided Data” means Personal Data  
371 provided to a Covered Entity directly by the Individual who is the  
372 subject of the Personal Data.

373 (1) Provided Data includes Personal Data provided by the Individual to  
374 the Covered Entity, such as—

375 (A) online or in-store transaction records, including credit or debit  
376 account information and contact information;

377 (B) account or event registration information;

378 (C) medical history given directly to a medical provider;

379 (D) password and answers to security questions entered to authenticate a  
380 user;

381 (E) response to a survey, questionnaire, contest, feedback form,  
382 comment field, or other inquiry or communication from the Covered  
383 Entity; or

384 (F) information submitted by an Individual as part of an application  
385 process or inquiry.

386 (2) Such term does not include Observed Data, Inferred Data, or Third-  
387 Party Provided Data.

388 (t) SENSITIVE PERSONAL DATA.—<sup>18</sup>The term “Sensitive Personal Data”  
389 means Personal Data that objectively and regardless of context, alone or

---

threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.” [NIST SP 800-12, Rev. 1, An Introduction to Information Security](#), Appendix B: Glossary, at p 30.

<sup>18</sup>The IAF Model’s definition of “Sensitive Data” is designed for a future-oriented, risk based legal framework. While it may be desirable to define some data as being more sensitive than other data, it is important to recognize

390 in combination with other data, presents a higher-than-average  
391 Processing Risk for an average Individual acting reasonably.

392 (1) Evidence of higher-than-average Processing Risk includes—

393 (A) USE.—There are numerous uses for the Personal Data, alone or in  
394 combination with other data, including unlawful or nefarious uses by  
395 a malicious actor, that may cause substantial Adverse Processing  
396 Impact.

397 (B) IDENTIFIABILITY AND LINKABILITY.—The Personal Data itself  
398 identifies an Individual or is directly linked or linkable to an  
399 Identifiable Individual.<sup>19</sup>

400 (C) AUTHENTICATION AND VERIFICATION.—The Personal Data is  
401 routinely used for identification, authentication, and verification of  
402 identity for commercial transactions, travel, employment, medical  
403 treatment, public benefits, education, and physical and logical  
404 access.

405 (D) LEGAL OBLIGATIONS.—The Personal Data is subject to statutory,  
406 regulatory, and other legal obligations or restrictions.

407 (E) PERMANENCE.—The Personal Data remains useful and relevant over  
408 time and cannot easily be replaced or substituted or is immutable.<sup>20</sup>

---

that it is more often than not the context in which data are used that creates real risks of inappropriate consequences. Unlike other bills which provide a finite list of categories of sensitive data, this definition focuses on the criteria and risk factors that make a given category of data “sensitive.” The model also provides an illustrative list of rebuttable presumptions that can be overcome in appropriate contexts. The criteria and risk factors are based, in part, on the criteria set forth in [Preparing for and Responding to a Breach of Personally Identifiable Information, OMB Memorandum M-17-12, January 3, 2017](#) .

<sup>19</sup> The IAF Model does not define “de-identified data,” “aggregate data,” “anonymous data,” or “pseudonymous data.” The focus of the analysis should be on the potential impact of the use of the data. Accordingly, the IAF Model does not exclude any of these categories of data from the definition of Personal Data or the coverage of the proposed law. Rather, the extent to which a given data set is identifiable is incorporated in the risk assessment. It is well understood today that even de-identified can and does have significant impacts on individuals, and therefore, de-identified data should not be excluded from a risk-based legal framework intended to promote beneficial innovation while limiting harmful outcomes. De-identification is a risk mitigation tool that should be part of an accountability and risk management program. Depending on the context, de-identified data and pseudonymous data can be Personal Data. This is consistent with the requirements in the General Data Protection Regulation (EU) 2016/679 ([GDPR](#)), and the current state of technology.

<sup>20</sup> This requirement includes an assessment of the relevancy and utility of the information over time and whether the information will permanently identify an individual. Some information loses its relevancy or utility as it ages, while other information is likely to apply to an individual throughout his or her life. For example, an individual's health

- 409 (F) PRIVACY EXPECTATION.—The Personal Data is reasonably  
410 considered highly personal, private, or of an intimate nature, and the  
411 average Individual takes steps to maintain the confidentiality of the  
412 Personal Data.
- 413 (2) A rebuttable presumption exists that the following Personal Data  
414 presents a higher-than-average Processing Risk for an average  
415 Individual acting reasonably—
- 416 (A) Biometric Data;
- 417 (B) social security numbers, passport numbers, driver’s license numbers,  
418 or any other unique government-issued identification number linked  
419 to a form of identification commonly used to identify, authenticate,  
420 or verify the identity of an Individual;
- 421 (C) unique account numbers together with any required security code,  
422 access code, or security question or password necessary to access an  
423 Individual’s account;
- 424 (D) Precise Geolocation Data;
- 425 (E) Personal Data related to an Individual’s physical, mental or  
426 behavioral health, including the provision of health care services;
- 427 (F) genetic data;<sup>21</sup>
- 428 (G) Personal Data related to an Individual’s sexual life, including sexual  
429 activity, sexual orientation, and/or sexual behavior;

---

insurance ID number can be replaced. However, information about an individual's health, such as family health history or chronic illness, may remain relevant for an individual's entire life, as well as the lives of his or her family members. Special consideration is warranted with biometric information including fingerprints, hand geometry, retina or iris scans, and DNA or other genetic information. When considering the nature and sensitivity of biometric information, a Covered Entity should factor in the known current uses of the information and consider that, with future advancements in science and technology, biometric information could have many additional uses not yet contemplated.

<sup>21</sup> Under the IAF Model, human biological material is not necessarily Personal Data. The analysis will depend on the context, including the intended use of the biological material. Consideration of context plays a central role in the IAF Model.

- 430 (H) calendar information, address book information, phone or text logs,  
431 photos or videos maintained in an Individual’s non-public account,  
432 whether on an Individual’s device or otherwise; and
- 433 (I) the content or metadata of an Individuals’ private communications  
434 and the identity of the parties to such communications, unless the  
435 Covered Entity is an intended party to a communication.
- 436 (u) SERVICE PROVIDER.—The term “Service Provider” means a person  
437 that—
- 438 (1) Processes Personal Data on behalf of and at the sole direction of a  
439 Covered Entity;
- 440 (2) may not Process such Personal Data except on instructions from the  
441 Covered Entity, unless otherwise required to do so by law; and
- 442 (3) may not disclose the Personal Data received from or on behalf of the  
443 Covered Entity, or any Personal Data derived from such Personal  
444 Data, other than as directed by the Covered Entity.
- 445 (v) THIRD PARTY.—The term “Third Party” means, with respect to any  
446 Covered Entity, a person that—
- 447 (1) is not a Service Provider; and
- 448 (2) is not related to the Covered Entity by common ownership or  
449 corporate control.
- 450 (w) THIRD-PARTY PROVIDED DATA.—The term “Third-Party Provided  
451 Data” means Personal Data provided to a Covered Entity from—
- 452 (1) an Individual other than the Individual who is the subject of the  
453 Personal Data;
- 454 (2) a Third Party;
- 455 (3) a government or any instrumentality of a government; or
- 456 (4) any other person.
- 457 (x) TRANSFER.—The term “transfer” means to disclose, release, share,  
458 disseminate, make available, sell, license, or otherwise communicate  
459 Personal Data by any means to a Third Party—
- 460 (1) in exchange for consideration; or

461 (2) for a commercial purpose.<sup>22</sup>

462  
463 **Article II. FAIR PROCESSING OF PERSONAL DATA**  
464 **Section 2.01 LAWFUL, RESPONSIBLE, AND FAIR**  
465 **PROCESSING.**

466 (a) **PERMISSIBLE PROCESSING.**—A Covered Entity may Process Personal  
467 Data when—

- 468 (1) the purpose of the Processing is for a specified legitimate use;
- 469 (2) the Processing is reasonably necessary and proportionate in relation to  
470 the purpose;
- 471 (3) the Covered Entity has performed a processing impact assessment as  
472 required by Article V of this Act and concluded that the Processing  
473 does not present an unacceptable level of Processing Risk; and
- 474 (4) the Covered Entity has developed, documented, and implemented  
475 reasonable and appropriate policies, processes, and procedures taking  
476 into account the specific purpose of the Processing and the level of  
477 Processing Risk.

478 (b) **LEGITIMATE USE.**—The Processing of an Individual’s Personal Data is  
479 legitimate only if and to the extent that a Covered Entity can  
480 demonstrate that one or more of the following applies—

- 481 (1) **COMPLIANCE WITH LEGAL OBLIGATIONS.**—The Individual’s  
482 Personal Data is Processed to—
- 483 (A) comply with a Federal, State, or local law, rule, or other applicable  
484 legal requirement; or
- 485 (B) comply with a civil, criminal, or regulatory inquiry, investigation,  
486 subpoena, civil investigative demand, or summons by Federal, State,  
487 or local authorities.
- 488 (2) **INFORMATION SECURITY.**—The Individual’s Personal Data is  
489 Processed to—

---

<sup>22</sup> This text is based on the definition of “transfer” in Brookings Institution’s proposed legislation, the [Information Privacy Act](#) – June 3, 2020. This definition does not include transfers to Service Providers or affiliates of the Covered Entity. Certain transfers by non-profit organizations may also be excluded.

- 490 (A) protect the confidentiality, integrity, and availability of data and the  
491 security of devices, networks, products, services, systems, data  
492 sources, or facilities against malicious and illegal activity, including  
493 to prevent, detect, or respond to cybersecurity incidents; or
- 494 (B) verify and authenticate the identity of an Individual, provided that  
495 Personal Data collected to verify and authenticate the identity of an  
496 Individual shall not be used for any other purpose.
- 497 (3) ROUTINE BUSINESS PROCESSES.—The Individual’s Personal Data is  
498 Processed to—
- 499 (A) support basic internal business functions that are necessary for a  
500 Covered Entity to operate, such as accounting, billing, payment  
501 processing, inventory and supply chain management, human  
502 resource management, quality assurance, and internal auditing;
- 503 (B) ensure correct and efficient operation of systems and processes,  
504 including to monitor, repair, and enhance performance, quality, or  
505 safety; or
- 506 (C) fulfill the terms of a written warranty or product recall conducted in  
507 accordance with Federal law.
- 508 (4) PROVIDE A REQUESTED PRODUCT OR SERVICE.—
- 509 (A) The Individual’s Personal Data is Processed to provide goods or  
510 services requested by an Individual to that Individual. In order to  
511 rely upon Paragraph 2.01(b)(4) as the basis for the legitimate use, the  
512 use must be Consistent with the Context of the relationship between  
513 the Individual and the Covered Entity.
- 514 (B) The use of Personal Data to provide a requested product or service  
515 includes the use to—
- 516 (i) render or operate a specific product or service used, requested, or  
517 authorized by the Individual;
- 518 (ii) provide the Individual with ongoing customer service, assistance,  
519 and technical support;



520 (iii) perform a contract to which the Individual is a party or take steps  
521 at the request of the Individual prior to entering into a contract; or  
522 (iv) complete the transaction for which the Personal Data was  
523 Processed.

524 (5) PROTECT AGAINST UNLAWFUL ACTIVITY.—The Individual’s  
525 Personal Data is Processed to—

526 (A) protect or defend the Covered Entity’s rights or property, including  
527 intellectual property, against actual or potential security threats,  
528 fraud, theft, unauthorized transactions, or other illegal activities;

529 (B) cooperate with law enforcement agencies concerning conduct or  
530 activity that the Covered Entity reasonably and in good faith believes  
531 may violate Federal, State, or local law; or

532 (C) exercise or defend legal claims.

533 (6) PUBLIC SAFETY AND HEALTH.—The Individual’s Personal Data is  
534 Processed to protect the health or safety of the Individual, a group of  
535 Individuals, or larger community, taking into account the totality of  
536 the circumstances pertaining to a particular threat.

537 (7) AFFIRMATIVE EXPRESS CONSENT.—An Individual has provided  
538 Affirmative Express Consent for the specific use.

539 (A) In order to rely upon Affirmative Express Consent as the basis for  
540 the legitimate use for Processing a Covered Entity shall—

541 (i) obtain Affirmative Express Consent from the Individual for the  
542 specific use before the Covered Entity begins Processing the  
543 Individual’s Personal Data; and

544 (ii) make available to the Individual a reasonable means to withdraw  
545 consent.

546 (B) To obtain Affirmative Express Consent, the description of the  
547 Processing for which consent is sought must be provided to the  
548 Individual in a standalone disclosure and must include a prominent  
549 heading identifying the Processing Activity or Activities for which  
550 consent is sought. Acceptance of a general or broad terms of use or

551 similar document that contains descriptions of Personal Data  
552 Processing along with other, unrelated information does not  
553 constitute Affirmative Express Consent.

554 (8) KNOWLEDGE DISCOVERY.<sup>23</sup>—The Individual’s Personal Data is  
555 Processed for internal research, investigation, and analysis designed to  
556 acquire knowledge, generate predictions, detect patterns, extract  
557 insights, identify anomalies, avoid errors, increase efficiency, and  
558 facilitate product improvement or development. To rely upon  
559 knowledge discovery as the legitimate use for Processing—

560 (A) the purpose of the Processing must be reasonably Consistent with the  
561 Context of the relationship between the Individual and the Covered  
562 Entity; and

563 (B) the Covered Entity must—

564 (i) identify knowledge discovery as the purpose of the specific  
565 Processing;

566 (ii) be able to demonstrate that the specific knowledge discovery  
567 cannot reasonably be performed without Personal Data and that the  
568 Personal Data being Processed is relevant and necessary for the  
569 particular Processing;

570 (iii) maintain on an ongoing basis a complete, accurate, and  
571 appropriately detailed inventory of specific knowledge discovery  
572 activities conducted across the Covered Entity;

---

<sup>23</sup> “Knowledge Discovery” is a new but essential concept, which is distinct from the more traditional concept of research. Processing of Personal Data for Knowledge Discovery draws an important distinction between (1) learning from data and (2) applying what has been learned. Knowledge Discovery may involve gathering data to be analyzed, pre-processing it into a format that can be used, consolidating it for analysis, analyzing it to discover what it may reveal and interpreting it to understand the processes by which the data was analyzed and how conclusions were reached. The conclusions or new knowledge learned during the Processing may not be applied to an activity, business process, decision-making, etc. that will impact an Individual unless there is a separate legitimate use. Given this restriction, Processing for Knowledge Discovery presents a different set of risks and considerations than other Processing. P. Bruening, [Advanced Data Analytic Processing](#) – 2019 Update, at 4.

- 573 (iv) prohibit the use or application of the result or outcome of  
574 Processing for knowledge discovery for any activities, measures,  
575 decisions, products, or services that may impact or relate to an  
576 Individual or group of Individuals, unless the Covered Entity can  
577 establish that the use or application of the result or outcome of the  
578 Processing fully satisfies the requirements for a separate and  
579 independent legitimate use as otherwise required by this Section;  
580 and
- 581 (v) designate a qualified employee who shall—
- 582 (a) be responsible and accountable for the specific knowledge  
583 discovery Processing Activity; and
- 584 (b) certify in writing on an annual basis that the Covered Entity is in  
585 compliance with the requirements of Section 2.01(b)(8) of this  
586 Act. Such certification shall be maintained by the Covered  
587 Entity and be available to demonstrate compliance with this Act.
- 588 (9) RESEARCH.—The Individual’s Personal Data is Processed for  
589 scientific analysis, systematic study, and observation, including basic  
590 research or applied research that is designed to develop or contribute  
591 to public or scientific knowledge and that adheres or otherwise  
592 conforms to all other applicable ethics and privacy laws, including but  
593 not limited to studies conducted in the public interest in the area of  
594 public health. In order to rely upon research as the legitimate use for  
595 Processing—
- 596 (A) the purpose of the Processing must be reasonably Consistent with the  
597 Context of the relationship between the Individual and the Covered  
598 Entity;
- 599 (B) the Covered Entity must be able to demonstrate that the research  
600 cannot reasonably be performed without Personal Data; and
- 601 (C) the Covered Entity must prohibit the use or application of the result  
602 or outcome of the research for any activities, measures, decisions,  
603 products, or services that may impact or relate to an Individual or

604 group of Individuals, unless the Covered Entity can establish that the  
605 use or application of the result or outcome of the research fully  
606 satisfies the requirements for a separate and independent legitimate  
607 use as otherwise required by this Section.

608 (10) ADVERTISING OR MARKETING PURPOSES.—The Individual’s  
609 Personal Data is Processed to disseminate a communication in any  
610 medium intended to induce an Individual to obtain goods, services, or  
611 employment, provided that a Covered Entity obtains Affirmative  
612 Express Consent from an Individual before using the Individual’s  
613 Sensitive Personal Data for Advertising or Marketing Purposes.<sup>24</sup>

614 (11) JOURNALISM.—The Individual’s Personal Data is Processed for the  
615 investigation and publication of newsworthy information of legitimate  
616 public concern to the public.

617 (c) REASONABLE BASIS.—It is unlawful and an independent and separate  
618 violation of this Act for a Covered Entity to rely upon a specific  
619 legitimate use as set forth in Section 2.01(b) of this Act for the purpose  
620 of complying with Section 2.01(a) of this Act without having a  
621 reasonable basis for such reliance or claim. The failure to conduct and  
622 document an investigation or analysis prior to Processing shall be  
623 evidence that a Covered Entity did not have a reasonable basis.

624 **Section 2.02 RESTRICTIONS ON PROCESSING.**

625 (a) EXTREME RISK.—Notwithstanding Section 2.01, a Covered Entity shall  
626 not Process Personal Data when the Processing is reasonably likely to  
627 produce an extreme level of Processing Risk, as defined in Section 5.03  
628 of this Act, unless, at a minimum—

- 629 (1) the Processing is expressly authorized by Federal or State statute;  
630 (2) the Covered Entity is in compliance with the applicable requirements  
631 of this Act; and

---

<sup>24</sup> Advertising and marketing, like other uses of personal data, are subject to a risk assessment. This is important given the increasingly diverse range of activities that often fall under the category of advertising or marketing in the information age. Moreover, as set forth in Article III, an individual may opt out of the sharing of personal data with third parties as well as the use of personal data for many, but not all, advertising and marketing purposes.

- 632 (3) the Covered Entity has obtained Affirmative Express Consent from  
633 the Individual before processing that Individual’s Personal Data,  
634 unless otherwise prohibited by law.
- 635 (b) HIGH RISK.—Notwithstanding Section 2.01(a), a Covered Entity shall  
636 not rely on Sections 2.01(b)(8), (9), or (10) as the legitimate use for  
637 Processing when the Processing is reasonably likely to produce a high  
638 or greater level of Processing Risk.
- 639 (c) NO UNDISCLOSED PROCESSING.—A Covered Entity shall not Process  
640 an Individual’s Personal Data unless the Covered Entity makes  
641 available to the Individual and the public the information required in  
642 Section 3.01 of this Act.

643  **Section 2.03 UNETHICAL AND RECKLESS**  
644 **PROCESSING.**

- 645 (a) It is unlawful and an independent and separate violation of this Act for  
646 a Covered Entity to Process Personal Data with reckless disregard for  
647 Processing Risk or for Adverse Processing Impact to the Individual.
- 648 (b) When determining if a Covered Entity engaged in Processing with such  
649 reckless disregard in a given context in violation of this Act, the  
650 following factors shall be considered—
- 651 (1) the Covered Entity’s intent to undertake the Processing that created  
652 the Processing Risk or caused the Adverse Processing Impact to the  
653 Individual;
- 654 (2) the foreseeability of the Processing Risk or the Adverse Processing  
655 Impact to the Individual;
- 656 (3) the closeness or proximity of the connection between the Processing  
657 and the severity of Adverse Processing Impact suffered by the  
658 Individual; and
- 659 (4) the extent to which the measures that could have been taken to  
660 mitigate Processing Risk were reasonably available or considered  
661 industry best practice at the time of the Processing.
- 662 (c) A Covered Entity may act with reckless disregard and thereby violate  
663 its legal duty to an Individual and this Act even if the Covered Entity

664 does not intend to cause Adverse Processing Impact. For the purposes  
665 of this Act, it is sufficient to establish that the Covered Entity intended  
666 to undertake the Processing that caused the Adverse Processing Impact  
667 to the Individual.  
668

669  **Article III. RESPONSIBILITIES OF ACCOUNTABLE COVERED**  
670 **ENTITIES**

671 **Section 3.01 OPEN AND TRANSPARENT PROCESSING.<sup>25</sup>**

672 (a) COMPREHENSIVE PUBLIC STATEMENT OF POLICIES AND PRACTICES.—

673 A Covered Entity shall publish and make readily available to the public  
674 on an ongoing basis a comprehensive statement about the Covered  
675 Entity’s Processing and an Individual’s options with regard to such  
676 Processing, including the following information—

- 677 (1) the identity of the Covered Entity, including any relevant affiliates,  
678 subsidiaries, or brands necessary to convey meaningful information to  
679 an Individual;
- 680 (2) the Covered Entity’s guiding principles for accountability and data  
681 responsibility as required by Section 4.01(b) of this Act;
- 682 (3) a description of the categories of Provided Data, Third-Party Provided  
683 Data, Observed Data, and Inferred Data Processed by the Covered  
684 Entity;
- 685 (4) a description of the categories of Sensitive Data Processed by the  
686 Covered Entity;
- 687 (5) for each category of Personal Data identified pursuant to paragraphs  
688 (a)(3) and (a)(4) above, a description of the use of the Personal Data

---

<sup>25</sup> The IAF believes transparency is very important. There should be no secret data systems. Transparency also adds to the ability for the market and regulators to govern fair behavior. IAF further believes that transparency for individuals and regulators should be two different communications devices. Accordingly, and as required in many other model bills, a Covered Entity must publish two notices: (1) a comprehensive statement for regulators and others interested in the details around Processing and (2) a summary statement for Individuals. A similar approach is codified in the model bills circulated by The Brookings Institution ([Information Privacy Act](#) – June 3, 2020 -2020.) and Consumer Reports ([Model State Privacy Bill](#)).

689 and purpose for Processing, unless the Processing is reasonably likely  
690 to create a high or greater level of Processing Risk, in which case, the  
691 Covered Entity shall provide a clear and detailed explanation of the  
692 specific use of the Personal Data and purpose for Processing;

693 (6) a statement identifying new or novel Processing Activities,  
694 applications of technology, or uses of Personal Data that are not yet  
695 widely deployed in a commercial context;<sup>26</sup>

696 (7) the length of time the Covered Entity intends to retain each category  
697 of Personal Data or, if that is not possible, the criteria used to  
698 determine such period, provided that a Covered Entity shall not retain  
699 an Individual’s Personal Data for longer than is reasonably necessary  
700 for the disclosed purpose for which the data was collected;<sup>27</sup>

701 (8) the specific purposes for which Personal Data may be Transferred to a  
702 Third Party and the categories of Third Parties who may receive such  
703 Personal Data;

704 (9) information regarding Automated Decision Making as required by  
705 Section 3.01(d) of this Act;

706 (10) an explanation of how an Individual may exercise each option  
707 available to the Individual with respect to the Processing of the  
708 Individual’s Personal Data as required by Sections 3.02, 3.04, 3.05,  
709 and 3.07 of this Act;

710 (11) any material changes to the Covered Entity’s Processing practices  
711 implemented in the preceding 12 months; and

712 (12) the effective date of the statement.

713 (b) MEANINGFUL SUMMARY EXPLANATION OF PROCESSING DIRECTED TO  
714 THE INDIVIDUAL.—A Covered Entity shall publish and make readily  
715 available to the public on an ongoing basis a summary of the Covered  
716 Entity’s Processing practices and activities. Such statement shall—

---

<sup>26</sup> A responsible and trustworthy organization affirmatively highlights new, novel, different or potentially surprising applications of technology or uses of personal data. An accountable organization should be transparent, truthful, and forthcoming with information about new or novel uses. This is not simply about deceptive omissions.

<sup>27</sup> This text is based on a similar provision in the [California Consumer Privacy Act of 2018](#) (“CCPA”).

- 717 (1) be drafted in a concise, intelligible, and easily accessible form using  
718 clear and plain language;
- 719 (2) be titled, “How We Process Your Personal Data;”
- 720 (3) identify the Covered Entity, including any relevant affiliates,  
721 subsidiaries, or brands necessary to convey meaningful information to  
722 an Individual;
- 723 (4) provide an Individual with a meaningful overview of the Processing of  
724 the Individual’s Personal Data;
- 725 (5) be provided to an Individual at or before the point when the Individual  
726 begins a transaction, orders a product or service, or otherwise  
727 commences a relationship with the Covered Entity and at or before the  
728 point when the Covered Entity collects Personal Data from the  
729 Individual, taking into account the nature of the interaction and the  
730 technology;<sup>28</sup>
- 731 (6) enable an Individual to make a reasonably informed decision  
732 regarding the Processing of the Individual’s Personal Data and the  
733 options available to the Individual; and
- 734 (7) link to the statement required in subsection (a) above.
- 735 (c) ADDITIONAL TRANSPARENCY AND ACCOUNTABILITY FOR HIGH  
736 RISK PROCESSING.—
- 737 (1) EXPLICIT NOTICE.—A Covered Entity shall provide explicit notice to  
738 an Individual prior to the collection from that Individual of Sensitive  
739 Personal Data or Personal Data that is reasonably likely to create a  
740 high or extreme level of Processing Risk under the circumstances.
- 741 (2) ENHANCED DISCLOSURES.—A Covered Entity shall conduct and  
742 document an analysis to determine if additional methods of notice and

---

<sup>28</sup> This requirement is similar to the requirement in the [CCPA regulations](#), that a business provide both a comprehensive privacy policy and a notice at collection, The purpose of the notice at collection is to provide consumers with timely notice, at or before the point of collection, about the categories of personal information to be collected from them and the purposes for which the personal information will be used.



743 communication are necessary to provide an Individual with clear,  
744 meaningful, relevant, and timely information regarding the Covered  
745 Entity’s Processing practices in a given context or circumstance. In  
746 conducting this analysis, a Covered Entity shall consider how an  
747 Individual may obtain such information and assert their preferences,  
748 including the extent to which an Individual has an opportunity to  
749 interact directly with information presented on a computer or mobile  
750 screen or similar mechanisms to configure preferences or exercise  
751 control over the way in which their Personal Data is Processed. Such  
752 analysis shall be incorporated in the processing impact assessment  
753 required by Section 5.04 of this Act and be conducted when—  
754 (A) the Covered Entity launches a new Processing Activity or makes  
755 material modifications to a current Processing Activity; and  
756 (B) the new or modified Processing Activity creates a high or extreme  
757 level of Processing Risk.

758 (d) TRANSPARENCY AND EXPLAINABILITY FOR AUTOMATED DECISION  
759 MAKING.—

760 (1) A Covered Entity shall establish one or more mechanisms to inform  
761 an Individual when Automated Decision Making may impact the  
762 Individual and the potential implications of such Automated Decision  
763 Making.

764 (2) The mechanism for providing the required information shall take into  
765 account the specific context of the Automated Decision Making and  
766 shall, to the extent practicable, provide the Individual with notice at  
767 the point of interaction.

768 (3) The notice shall, at a minimum, be designed to—  
769 (A) make an Individual aware of the Individual’s interaction with  
770 Automated Decision Making;  
771 (B) enable an Individual to understand the purpose of the Automated  
772 Decision Making; and

773 (C) enable an Individual adversely affected by the use of or reliance on  
774 Automated Decision Making to challenge the Automated Decision  
775 Making pursuant to Section 3.05(b) of this Act.

776

777  **Section 3.02 MEANINGFUL CONTROL.<sup>29</sup>**

778 (a) DISCONTINUE THIRD-PARTY TRANSFERS.—

779 (1) A Covered Entity shall provide an Individual with a means to request  
780 that a Covered Entity that Transfers Personal Data about the  
781 Individual to Third Parties stop Transferring the Individual’s Personal  
782 Data. A Covered Entity that has received a verified request from an  
783 Individual to stop Transfers of the Individual’s Personal Data shall be  
784 prohibited from Transferring the Individual’s Personal Data after its  
785 receipt of the Individual’s request unless the Individual subsequently  
786 provides Affirmative Express Consent for the Transfer.

787 (2) RULEMAKING.—<sup>30</sup>

788 (A) IN GENERAL.—Not later than 18 months after the date of enactment  
789 of this Act, the Commission shall issue a rule under section 553 of  
790 title 5, United States Code, establishing one or more acceptable  
791 processes for Covered Entities to follow in allowing an Individual to  
792 discontinue Transfers of the Individual’s Personal Data.

793 (B) REQUIREMENTS.—The processes established by the Commission  
794 pursuant to this subsection shall—

795 (i) be centralized, to the extent feasible, to minimize the number of  
796 requests of a similar type that an Individual must make;

---

<sup>29</sup> The IAF Model captures the controls that come from other regimes and proposals, evolves them for today’s more complex data world, and merges them with the flexibility that has fostered innovation in the United States. The obligations on a Covered Entity and corresponding mechanisms for an Individual to exert control over data use and submit requests set forth in Article III must be read in conjunction with the specific and general exceptions in Article III. As with all proposed frameworks, there are reasonable limitations on an Individual’s ability to access Personal Data and opt out of Processing. The exceptions in the IAF Model are generally consistent with most other draft bills and the [CCPA](#).

<sup>30</sup> This text aligns with the opt-out and rulemaking provisions in Section 104(a) of the Brookings Institution’s proposed legislation, the [Information Privacy Act](#) – June 3, 2020.

- 797 (ii) permit an Individual to authorize another person to submit a  
798 request on the Individual’s behalf;
- 799 (iii) include clear and conspicuous discontinuation notices and  
800 consumer-friendly mechanisms to allow an Individual to  
801 discontinue Transfers of Personal Data;
- 802 (iv) allow an Individual who objects to a Transfer of Personal Data to  
803 view the status of such objection;
- 804 (v) allow an Individual who objects to a Transfer of Personal Data to  
805 withdraw or modify such objection; and
- 806 (vi) be informed by the Commission’s experience developing and  
807 implementing the National Do Not Call Registry and researching  
808 technical mechanisms for expressing choice in other contexts.
- 809 (b) OPT OUT OF USE OF PERSONAL DATA.—
- 810 (1) A Covered Entity shall provide an Individual with a means to request  
811 that a Covered Entity that Processes Personal Data about the  
812 Individual stop using the Individual’s Personal Data. A Covered  
813 Entity that has received a verified request from an Individual to stop  
814 using the Individual’s Personal Data shall be prohibited from using the  
815 Individual’s Personal Data after its receipt of the Individual’s request  
816 unless the Individual subsequently provides Affirmative Express  
817 Consent.
- 818 (2) LIMITED EXCEPTION TO OPT OUT FOR CERTAIN ADVERTISING AND  
819 MARKETING.<sup>31</sup>—A Covered Entity may continue to use an  
820 Individual’s Personal Data following a request pursuant to  
821 paragraph (b)(1) for advertising and marketing purposes on websites,  
822 applications, or services owned and operated by the Covered Entity to  
823 the extent that—
- 824 (A) the specific use is Consistent with the Context of the Relationship  
825 between the Individual and the Covered Entity; and


---

<sup>31</sup> The scope of this narrow exception is similar to the list of activities not considered to be targeted advertising under Virginia’s new [Consumer Data Protection Act](#) .


- 826 (B) the advertising or marketing are not based on either—
- 827 (i) Processing the Individual’s Personal Data over time and across
- 828 unaffiliated websites, applications, or services; or
- 829 (ii) Sensitive Personal Data, unless the Covered Entity has obtained
- 830 Affirmative Express Consent for the specific advertising or
- 831 marketing use.
- 832 (c) DELETION OF PERSONAL DATA.—<sup>32</sup>A Covered Entity shall provide an
- 833 Individual with a mechanism to request that the Covered Entity delete
- 834 the Individual’s Personal Data. In response to a verified request to
- 835 delete Personal Data, the Covered Entity shall, to the extent practicable,
- 836 delete such data from its records or the technical equivalent, and direct
- 837 any Service Providers to delete the Individual’s Personal Data from
- 838 their records or the technical equivalent. A Covered Entity may satisfy
- 839 this requirement by permanently disposing, deleting, destroying,
- 840 purging, wiping or removing data elements from a data set such that the
- 841 remaining data or data set no longer identifies, relates to, describes, is
- 842 reasonably capable of being associated with, could reasonably be
- 843 linked, directly or indirectly, with a particular Individual.
- 844 (d) EXCEPTIONS.—A Covered Entity shall not be required to comply with
- 845 an Individual’s request pursuant to this Section to the extent that—
- 846 (1) the Individual’s Personal Data is necessary for the legitimate uses
- 847 identified in Sections 2.01(b)(1)–2.01(b)(6); or
- 848 (2) the Individual’s Personal Data is necessary to continue ongoing
- 849 research as provided for in Section 2.01(b)(9) and honoring the
- 850 Individual’s request will render impossible or seriously impair the
- 851 ability to complete such research.

---

<sup>32</sup> The opportunity for an Individual to request deletion of Personal Data under the IAF Model does not, and is not intended to, mirror the right to erasure (“right to be forgotten”) under [GDPR](#).

- 852  (e) SUBVERTING CHOICE AND MEANINGFUL CONTROL PROHIBITED.<sup>33</sup>—It  
853 is unlawful and a separate and independent violation of this Act for a  
854 Covered Entity to—
- 855 (1) knowingly design, modify, or manipulate a user interface with the  
856 purpose or substantial effect of obscuring, subverting, or impairing  
857 user autonomy, decision-making, or choice to obtain consent or  
858 Personal Data;
  - 859 (2) impersonate any entity or Individual in order to collect Personal Data  
860 or obtain access to an Individual account or device, including but not  
861 limited to a financial, medical, email, internet, social media, or  
862 telecommunications account; or
  - 863 (3) misrepresent or mischaracterize any product or service in order to  
864 induce the disclosure of Personal Data.

865

866  **Section 3.03 DATA QUALITY, ACCURACY, AND**  
867 **RETENTION.**

- 868 (a) A Covered Entity shall keep Personal Data Processed by the Covered  
869 Entity reasonably accurate, complete, and current. In determining  
870 whether Personal Data is reasonably accurate, complete, and current in  
871 a given context, a Covered Entity shall consider, at a minimum—
  - 872 (1) the sensitivity of the Personal Data;
  - 873 (2) the legitimate use of the Personal Data; and
  - 874 (3) the level of Processing Risk.
- 875 (b) A Covered Entity shall implement reasonable procedures to track  
876 updates or changes to Personal Data over time.
- 877 (c) A Covered Entity shall not maintain Personal Data once the Personal  
878 Data is no longer reasonably necessary for a legitimate use. A Covered

---

<sup>33</sup> An ethical, trustworthy, and accountable organization should take proactive measures to make choices simple and straightforward for consumers. This text is based upon [CPRA](#), which prohibits so-called “dark patterns.” This was first addressed in the [Deceptive Experiences to Online Users Reduction Act](#) (DETOUR Act), introduced by Senators Mark Warner (D-VA) and Joni Ernst (R-IA). The [SAFE DATA Act](#), and the Consumer Reports [Model State Privacy Act](#) include similar language.

879 Entity may satisfy this requirement by permanently disposing, deleting,  
880 destroying, purging, wiping, or removing data elements from a data set  
881 such that the remaining data or data set no longer identifies, relates to,  
882 describes, is reasonably capable of being associated with, could  
883 reasonably be linked, directly or indirectly, with a particular Individual.

884  **Section 3.04 ACCESS AND DATA PORTABILITY.**


885 (a) ACCESS TO PERSONAL DATA.—A Covered Entity shall provide an  
886 Individual with a mechanism to request access to the Individual’s  
887 Personal Data. Upon receiving a verified request from an Individual, a  
888 Covered Entity shall provide the Individual with confirmation as to  
889 whether or not the Covered Entity is Processing Personal Data about the  
890 Individual and, when the response is in the affirmative, shall provide  
891 the Individual with reasonable access to the Individual’s Personal Data  
892 retained by the Covered Entity as follows—

- 893 (1) Provided Data;
- 894 (2) Third-Party Provided Data, including information as to the source of  
895 the Personal Data, where practicable;
- 896 (3) with respect to Observed Data—
- 897 (A) a list of the specific categories of data that have been observed about  
898 the Individual;
- 899 (B) the specific purpose and legitimate use for Processing each of the  
900 specific categories of Observed Data; and
- 901 (C) the level of Processing Risk assigned to the Observed Data or  
902 relevant Processing Activity.
- 903 (4) with respect to Inferred Data—
- 904 (A) a list of the specific categories of Inferred Data about the Individual;
- 905 (B) the specific purpose and legitimate use for Processing each of the  
906 specific categories of Inferred Data;
- 907 (C) the reasonably anticipated consequences of such Processing and the  
908 level of Processing Risk assigned to the Inferred Data or relevant  
909 Processing Activity; and

910 (D) where the Processing of the Inferred Data creates a moderate or  
911 greater level of Processing Risk, meaningful information about the  
912 process or methodology employed to create the Inferred Data.

913 (b) STATEMENT OF ACCOUNTABILITY IN LIEU OF ACCESS.—

914 (1) Where a Covered Entity can demonstrate that it is unduly  
915 burdensome, technically infeasible, and not practicable to provide an  
916 Individual with access to all or a subset of the Individual’s Personal  
917 Data as otherwise required by this Act and has determined with a high  
918 degree of certainty that the Processing does not create a high or  
919 extreme level of Processing Risk, a Covered Entity may provide an  
920 Individual with a written statement explaining the reasons that access  
921 cannot be provided and confirming that the Processing of the  
922 Individual’s Personal Data is subject to internal policies, processes,  
923 and procedures for the Processing of Personal Data necessary to  
924 ensure lawful, responsible, and accountable Processing given the  
925 intended uses of the data and the level of Processing Risk.

926  (2) It shall be unlawful and a separate violation of this Act for a Covered  
927 Entity to rely upon Section 3.04(b) of this Act in bad faith or provide a  
928 statement as required in Section 3.04(b) of this Act that is false,  
929 misleading, or inaccurate.

930 (c) ACCESS TO INFORMATION ABOUT TRANSFERS TO THIRD PARTIES.—A  
931 Covered Entity shall provide an Individual with a mechanism to request  
932 a list identifying the Third Parties with whom the Covered Entity  
933 Transfers the Individual’s Personal Data. Upon receiving a verified  
934 request from an Individual, a Covered Entity shall provide the  
935 Individual with a list identifying the specific category or categories of  
936 Third Parties with whom the Covered Entity Transfers the Individual’s  
937 Personal Data, unless the Processing is reasonably likely to create a  
938 high or extreme level of Processing Risk, in which case the Covered  
939 Entity shall provide the Individual with a list identifying the specific  
940 Third Parties with whom the Covered Entity Transfers or has

941 Transferred the Individual’s Personal Data and the purpose for such  
942 Transferring.

943 (d) DATA PORTABILITY.<sup>34</sup>

944 (1) A Covered Entity shall provide an Individual with a mechanism to  
945 request that the Covered Entity provide the Individual with copies of  
946 their Personal Data in a readily usable, portable format.

947 (2) PROVIDED DATA.—Upon receiving a verified request from an  
948 Individual, a Covered Entity shall, where technically feasible, make  
949 available a reasonable means for an Individual to transmit or Transfer  
950 Provided Data about the Individual retained by the Covered Entity to  
951 another Covered Entity in a structured, standardized, machine-  
952 readable, interoperable format, or otherwise download Personal Data  
953 in a readily usable format for the Individual’s own use.

954 (3) THIRD-PARTY PROVIDED DATA, OBSERVED DATA, AND INFERRED  
955 DATA.—A Covered Entity may decline to provide an Individual with  
956 the ability to Transfer, transmit, or download Personal Data, as  
957 specified in Section 3.04(d), for Third-Party Provided Data, Observed  
958 Data or Inferred Data if the Transfer, transmission, or download of  
959 such data could—

960 (A) reasonably be expected to reveal confidential, proprietary or trade  
961 secret information, or other intellectual property; or

962 (B) provide a competitor with the benefit or value of Processing  
963 undertaken by the Covered Entity to the disadvantage of the Covered  
964 Entity.

---

<sup>34</sup> In contrast with access, correction, deletion, and other provisions in Article III, data portability is concerned primarily with competition. The [Introduction to the Consumer Reports Model State Privacy Act](#), explains that data portability “requires companies to provide data in a format that could be easily transferred to a competing service, helping to improve competition among online services.” Accordingly, different considerations and policy decisions inform the scope and desirability of the requirement. IAF has not conducted research regarding data portability or competition issues.



- 965 (e) BUSINESS CONTINUITY PLAN.—A Covered Entity shall identify those  
966 circumstances in which the inability of an Individual to access the  
967 Individual’s Personal Data is reasonably likely to create a high or  
968 extreme level of Processing Risk. Where such Processing Risk exists, a  
969 Covered Entity shall develop, document, and implement an appropriate  
970 business continuity plan in order to ensure services and access can be  
971 reasonably maintained and restored as appropriate.
- 972 (f) EXCEPTIONS.—A Covered Entity shall not be required to make  
973 Personal Data available pursuant to this Section if—
- 974 (A) such access is limited by law, legally recognized privilege, or other  
975 legal obligation;
- 976 (B) the Individual’s Personal Data is—
- 977 (i) necessary for the legitimate uses identified in Sections 2.01(b)(2)  
978 or 2.01(b)(5); and
- 979 (ii) making the Personal Data available would be inconsistent with or  
980 undermine with such use; or
- 981 (C) the Personal Data—
- 982 (i) was previously deleted by the Covered Entity in compliance with  
983 documented data retention schedules;
- 984 (ii) constitutes confidential commercial information or trade secrets,  
985 including an algorithm used to make predictions, inferences,  
986 scores, or other decisions; or
- 987 (iii) a Covered Entity makes an individualized determination that  
988 fulfilling the request from the Individual would create Processing  
989 Risk or legitimate risk to the security, safety, free expression, or  
990 other rights of another Individual.

991  **Section 3.05 RESPONSIBLE AND ACCESSIBLE**  
992 **REDRRESS.**

- 993 (a) CORRECTION OF PERSONAL DATA.—A Covered Entity shall, consistent  
994 with the requirements and exceptions in Section 3.04 of this Act,  
995 provide an Individual with a mechanism to dispute and resolve the  
996 accuracy or completeness of Personal Data. Upon receipt of a verifiable

997 request, a Covered Entity shall make commercially reasonable efforts to  
998 correct the inaccurate Personal Data.

999 (b) CHALLENGE AUTOMATED DECISION MAKING.—A Covered Entity shall  
1000 provide an Individual with a mechanism to challenge Automated  
1001 Decision Making when the Individual has reason to believe that the  
1002 Individual suffered or is likely to suffer Adverse Processing Impact as a  
1003 result of the Automated Decision Making.

1004 (c) COMPLAINT PROCESS.—A Covered Entity shall provide an Individual  
1005 with a mechanism to submit a complaint or inquiry regarding a Covered  
1006 Entity’s policies, processes, and procedures relating to the Processing of  
1007 the Individual’s Personal Data or compliance with this Act.

1008 (d) ADDITIONAL REDRESS MECHANISMS FOR HIGH RISK PROCESSING.—  
1009 A Covered Entity with annual revenue in excess of \$100 million shall  
1010 conduct and document an analysis before commencing any Processing  
1011 Activity that creates a high or extreme level of Processing Risk in order  
1012 to determine if additional or special redress mechanisms are warranted  
1013 given the nature and scope of the Covered Entity’s activities and data  
1014 holdings. Such analysis shall be incorporated in the processing impact  
1015 assessment required by Article V of this Act.



**Section 3.06 DATA SECURITY.**<sup>35</sup>

1017 (a) A Covered Entity shall develop, document, and implement a  
1018 comprehensive data security program that includes administrative,  
1019 technical, and physical safeguards to protect the confidentiality,  
1020 integrity, and availability of Personal Data.<sup>36</sup> Such program shall be  
1021 appropriate to the Covered Entity’s size and complexity, the nature and  
1022 scope of the Covered Entity’s activities, the nature of Personal Data  
1023 Processed by the Covered Entity, and the level of Processing Risk.

---

<sup>35</sup> The IAF Model does not address data breach notification.

<sup>36</sup> Like Article 32 of the [GDPR](#), the IAF Model recognizes encryption as a security technique that may help keep personal data safe, but does not state that encrypted data is no longer personal data; nor does the IAF model state that encrypted data is not governed by the law.

- 1024 (b) In order to develop, document, and implement a data security program,  
1025 a Covered Entity shall—
- 1026 (1) identify reasonably foreseeable internal and external risks to the  
1027 confidentiality, integrity, and availability of Personal Data that could  
1028 result in the unauthorized access, disclosure, use, alteration,  
1029 destruction, or other compromise of such data, and assess the  
1030 sufficiency of any safeguards in place to control these risks;
- 1031 (2) maintain ongoing awareness of data security, vulnerabilities, threats,  
1032 and incidents;
- 1033 (3) develop, document, and implement incident management policies,  
1034 processes, and procedures that address incident detection, response,  
1035 and recovery;
- 1036 (4) develop, document, and implement safeguards to control reasonably  
1037 foreseeable risks through risk assessment and regularly test or  
1038 otherwise monitor the effectiveness of the safeguards’ key policies,  
1039 processes, and procedures; and
- 1040 (5) evaluate and adjust the Covered Entity’s data security program in light  
1041 of the results of the testing and monitoring, material changes to  
1042 operations or business arrangements, or other circumstances that may  
1043 have a material impact on the Covered Entity’s data security program.



**Section 3.07 PROCEDURES, EXCEPTIONS, AND RULE  
OF CONSTRUCTION.**

- 1046 (a) REASONABLE PROCEDURES.—
- 1047 (1) A Covered Entity shall make available a reasonably accessible,  
1048 conspicuous, and easy-to-use means for an Individual to exercise, at  
1049 no cost to the Individual, each option required by Article III of this  
1050 Act.
- 1051 (2) A Covered Entity shall honor an Individual’s request pursuant to  
1052 Sections 3.02(a) and 3.02(b) of this Act without undue delay and no  
1053 later than 7 business days following the request.
- 1054 (3) With respect to a request or complaint filed by an Individual pursuant  
1055 to Sections 3.02(c), 3.04(a), 3.04(c), 3.04(d), 3.05(a), 3.05(b), and


1056 3.05(c) of this Act, a Covered Entity shall respond to the Individual  
1057 without undue delay and no later than 30 days after receiving the  
1058 request or complaint. The Covered Entity shall provide the Individual  
1059 with sufficient information to understand and act upon the response.

1060 (4) A Covered Entity shall establish an internal process whereby  
1061 Individuals may appeal a refusal to take action on a request made  
1062 pursuant to Article III of this Act within a reasonable period of time  
1063 after the Individual's receipt of the response sent by the Covered  
1064 Entity as required by Section 3.07 of this Act. The appeal process  
1065 must be conspicuously available and as easy to use as the process for  
1066 submitting such a request under Section 3.07 of this Act.

1067 (b) EXCEPTIONS.—

1068 (1) A Covered Entity shall not be required to comply with Sections  
1069 3.01(d), 3.02(c), 3.04(a), 3.04(c), 3.04(d), 3.05(a), and 3.05(b) of this  
1070 Act if the Covered Entity determines with a reasonable degree of  
1071 certainty, after completing and documenting a processing impact  
1072 assessment pursuant to Article V of this Act, that the Processing will  
1073 create no more than a very low level of Processing Risk.

1074 (2) A Covered Entity shall not be required to comply with a request from  
1075 an Individual or to respond to an Individual's complaint or inquiry if  
1076 the Covered Entity has reason to believe and can demonstrate that  
1077 such request, complaint, or inquiry is frivolous, vexatious, and in bad  
1078 faith.

1079  (3) If a Covered Entity relies on an exception provided for in Title III of  
1080 this Act, the Covered Entity bears the burden of demonstrating that the  
1081 Covered Entity qualifies for the exception. It is unlawful and an  
1082 independent and separate violation of this Act for a Covered Entity to  
1083 rely upon a specific exception as set forth in this Section without  
1084 having a reasonable basis for such reliance.

1085 (4) Journalism Exception.—With the exception of Section 3.06, nothing  
1086 in this Article shall apply to the publication of newsworthy

1087 information of legitimate public concern to the public by a Covered  
1088 Entity, or to the processing or Transfer of information by a Covered  
1089 Entity for that purpose.<sup>37</sup>

1090 (c) RULE OF CONSTRUCTION.—Nothing in this Act shall be construed to  
1091 require a Covered Entity to—

1092 (1) take an action that would convert information that is not Personal Data  
1093 into Personal Data; or

1094 (2) delete, destroy, or de-identify data that is retained for backup or  
1095 archival purposes to the extent that such systems are not and cannot be  
1096 accessed in the ordinary course.

1097 (d) WAIVER.—The options available to Individuals and remedies provided  
1098 under Article III of this Act may not be waived or limited by contract or  
1099 otherwise.

1100 (e) RULEMAKING.—The Commission shall, within 1 year of enactment of  
1101 this Act and in accordance with section 553 of title 5, United States  
1102 Code, promulgate regulations to—

1103 (1) modify or add additional exceptions and limitations to the  
1104 requirements set forth in Article III;

1105 (2) identify the categories of Personal Data, Sensitive Personal Data, and  
1106 Third Parties that Covered Entities must identify pursuant to Section  
1107 3.01 and 3.04; and

1108 (3) establish reasonable requirements for a Covered Entity to verify the  
1109 identity of an Individual when submitting a request to a Covered  
1110 Entity pursuant to Article III of this Act.

1111

## 1112 **Article IV. ACCOUNTABLE PROCESSING<sup>38</sup>**

---

<sup>37</sup> The Journalism Exception is from the Brookings Institution’s proposed legislation, the [Information Privacy Act](#) – June 3, 2020, All bills have a similar exception for freedom of the press and speech protected by the [First Amendment of the Constitution](#) .

<sup>38</sup> Interoperability of legal frameworks is one of the objectives of the IAF Model. To that end, it is relevant to highlight that the principle of accountability is one of the central pillars of the [GDPR](#). GDPR Article 5(2), Like the IAF Model, the accountability requirements place responsibility firmly on the controller (Covered Entity) to take proactive action to achieve compliance and to be ready to demonstrate that compliance. The IAF Model, however, provides more detail to help organizations meet their obligations and to help regulators enforce the law in a

1113  
1114  
1115  
1116  
1117  
1118  
1119  
1120  
1121  
1122  
1123  
1124  
1125  
1126  
1127  
1128  
1129  
1130  
1131  
1132  
1133  
1134  
1135  
1136  
1137  
1138  
1139  
1140  
1141



**Section 4.01 ACCOUNTABLE PROCESSING  
MANAGEMENT PROGRAM.**

- (a) PURPOSE.—A Covered Entity shall develop, document, and implement an accountable processing management program to—
  - (1) comply with the requirements of this Act, other applicable legal or regulatory requirements, and recognized industry practices;
  - (2) promote structured, effective, and consistent management and oversight of Processing across the Covered Entity;
  - (3) evaluate Processing Risk and the impacts of Processing on Individuals and competition and consider the interests of all relevant stakeholders when making determinations about Processing;
  - (4) manage risk, including Processing Risk, on an ongoing basis; and
  - (5) demonstrate the Covered Entity’s ongoing commitment to trustworthy, fair, responsible, and transparent Processing.
- (b) GUIDING PRINCIPLES FOR ACCOUNTABILITY AND DATA RESPONSIBILITY.—
  - (1) ESTABLISH STRATEGIC VISION.—A Covered Entity shall define, document, and publish guiding principles regarding Processing that identify, at a minimum, a Covered Entity’s top-level goals and objectives, values, and strategic vision with respect to data stewardship, data ethics, responsible Processing, and accountability. The guiding principles should extend beyond meeting minimum regulatory requirements.
  - (2) SENIOR MANAGEMENT REVIEW AND APPROVAL.—The Board of Directors or equivalent senior governing body of a Covered Entity shall review and approve the guiding principles on an annual basis and require all Processing across the Covered Entity to align with the Covered Entity’s guiding principles for accountability and data responsibility.

---

consistent and predictable fashion. Similarities with the IAF Model may also be found in the [Singapore Personal Data Protection Act 2012](#), which places a significant emphasis on accountability.

- 1142 (c) PROGRAM DEVELOPMENT AND IMPLEMENTATION.—An accountable  
1143 processing management program shall include—
- 1144 (1) a qualified senior executive to oversee the development,  
1145 documentation, and implementation of the program;
- 1146 (2) strategic planning that considers across the Covered Entity both  
1147 Personal Data itself and related resources, such as personnel,  
1148 equipment, funds, and information technology;
- 1149 (3) ongoing collaboration between designated senior executives across  
1150 different functions and lines of business to ensure coordination of risk  
1151 management, business operations, legal and regulatory compliance,  
1152 security, and Processing Activities;
- 1153 (4) documentation demonstrating that a Covered Entity has an  
1154 accountable Processing management program in place and the  
1155 capacity to comply with legal and program requirements on an  
1156 ongoing basis. Such documentation shall provide an overview of the  
1157 program, including a description of the—
- 1158 (A) management and structure of the program;  
1159 (B) resources dedicated to the program;  
1160 (C) role and authority of designated accountable officials and staff; and  
1161 (D) strategic goals and objectives of the program; and
- 1162 (5) resources, staff, policies, processes, and procedures that are reasonable  
1163 and appropriate to—
- 1164 (A) a Covered Entity’s size and complexity;  
1165 (B) the nature and scope of a Covered Entity’s activities;  
1166 (C) legal requirements and obligations that apply to such activities;  
1167 (D) the scale of a Covered Entity’s Processing operations; and  
1168 (E) the sensitivity of Personal Data Processed and the level of  
1169 Processing Risk created by the Covered Entity’s Processing  
1170 Activities.
- 1171 (d) RESPONSIBLE DATA GOVERNANCE.—As part of an accountable  
1172 processing management program, a Covered Entity shall—

- 1173 (1) establish policies, processes, and procedures to ensure that Personal  
1174 Data is managed and maintained according to applicable laws,  
1175 industry codes of conduct, recognized industry practices, and the  
1176 requirements of the accountable management program;
- 1177 (2) properly and consistently manage Personal Data as required by  
1178 policies, processes, and procedures throughout its lifecycle, including  
1179 all stages of Processing, such as creation, collection, use, analysis,  
1180 storage, maintenance, dissemination, disclosure, Transfer, and  
1181 disposition;
- 1182 (3) identify, distinguish, and manage different categories of Personal Data  
1183 and Personal Data obtained, collected, received, or created from  
1184 different sources, including Provided Data, Third-Party Provided  
1185 Data, Observed Data , and Inferred Data;
- 1186 (4) classify Personal Data, including Sensitive Personal Data;
- 1187 (5) designate an accountable employee who can reliably describe how  
1188 Personal Data is Processed throughout each Processing Activity; and
- 1189 (6) maintain a current, complete, and accurate inventory of the Covered  
1190 Entity’s information systems and information holdings, including the  
1191 Covered Entity’s information systems that Process Personal Data.

1192  **Section 4.02 ETHICAL, TRUSTWORTHY, AND**  
1193 **PREVENTATIVE DESIGN.<sup>39</sup>**

- 1194 (a) PROGRAM OBJECTIVES.—When developing a new Processing Activity  
1195 or updating an existing Processing Activity, a Covered Entity shall  
1196 consider, evaluate, and integrate, as appropriate, technical and  
1197 nontechnical processes, engineering analyses, design principles, and  
1198 controls in order to build and deliver a more trustworthy Processing  
1199 Activity and minimize adverse effects, including Processing Risk.
- 1200 (b) CORE REQUIREMENTS.—A trustworthy Processing Activity shall seek  
1201 to—

---

<sup>39</sup> This approach generally aligns with [GDPR](#), Article 25, Data Protection by Design and By Default, and the new relevant guidance, EDPB 2020A: European Data Protection Board, [Guidelines on Article 25 Data Protection by Design and by Default](#) (Version 2.0, 20 October 2020),



- 1202 (1) enable reliable assumptions by the Covered Entity, Individuals, and  
1203 other entities about data and data Processing in a given Processing  
1204 Activity; and
- 1205 (2) meet the specific Processing requirements for each Processing Action  
1206 such that the outcome or result of the Processing Activity is  
1207 predictable and is capable of mitigating Processing Risk as anticipated  
1208 and required.
- 1209 (c) PLANNING FOR TRUSTWORTHY DESIGN.—A Covered Entity shall,  
1210 during the initial stages of any development process and throughout the  
1211 various stages of the Processing Activity development lifecycle—
- 1212 (1) inventory, incorporate, and apply the legal rules, industry best  
1213 practices, contractual obligations, and internal requirements for the  
1214 Processing of Personal Data as well as for anticipating and facilitating  
1215 implementation of controls that may be necessary to support  
1216 compliance;
- 1217 (2) identify discrete Processing Actions within a given Processing  
1218 Activity and determine which data Processing Actions may create  
1219 Processing Risk and assess the level of Processing Risk;
- 1220 (3) develop, document, and implement a repeatable and measurable  
1221 decision-making process that covers the life of each Processing  
1222 Activity and includes explicit criteria for analyzing the benefits and  
1223 risks, including information security and Processing Risk, associated  
1224 with each stage in the lifecycle of both Personal Data and supporting  
1225 technologies; and
- 1226 (4) consider and document the impact of decisions and actions in each  
1227 stage of the lifecycle.
- 1228 (d) ASSESS AND IMPLEMENT REQUIREMENTS.—For each Processing  
1229 Activity, a Covered Entity should—
- 1230 (1) determine the need or desirability for the Covered Entity to have the  
1231 capability to review, identify, access, Transfer, segregate, tag, track,  
1232 retrieve, alter, delete, and otherwise manage Personal Data;

- 1233 (2) integrate the required or desired capabilities into the design to the  
1234 extent practicable;
- 1235 (3) manage or administer Personal Data with sufficient granularity in  
1236 order to provide confidence that inaccurate Personal Data can be  
1237 identified and corrected, obsolete Personal Data is disposed of,  
1238 Personal Data is Processed only for legitimate uses, and an  
1239 Individual’s preferences about use and Transfer of their Personal Data  
1240 are implemented and maintained;
- 1241 (4) conduct technical, process, and risk analyses of alternative design  
1242 implementations in order to reduce risk and increase accountability;
- 1243 (5) consider how a given system can be audited such that it is possible to  
1244 trace any access to the information system, modifications made, and  
1245 any action carried out in order to identify its author;
- 1246 (6) avoid the use of Personal Data for testing Processing Activities to the  
1247 extent feasible and implement controls to mitigate Processing Risk if  
1248 Personal Data must be used;
- 1249 (7) enable the Processing of data without association to Individuals or  
1250 devices beyond the operational requirements of the Processing  
1251 Activity through technical methods such as de-identification and rule-  
1252 based restrictions on Processing; and
- 1253 (8) develop public facing mechanisms for an Individual to interact with  
1254 the Processing Activity or exercise choices as required by Article III  
1255 of this Act that—
- 1256 (A) are clear and easy-to-use;
- 1257 (B) are designed to reduce the burden on an Individual;
- 1258 (C) would meet the expectations of a reasonable Individual; and
- 1259 (D) do not have the substantial effect of subverting or impairing user  
1260 autonomy, decision-making, or choice.

1261  **Section 4.03 ACCOUNTABILITY FOR AUTOMATED**  
1262 **DECISION MAKING**

- 1263 (a) GENERAL OBLIGATIONS FOR THE TRUSTWORTHY AND ACCOUNTABLE  
1264 USE OF AUTOMATED DECISION MAKING.—A Covered Entity that

1265 relies upon or uses Automated Decision Making to make or inform a  
1266 decision or incorporates Automated Decision Making at any point in a  
1267 decision making process shall—

- 1268 (1) understand the reasoning behind the Automated Decision Making;
- 1269 (2) exercise judgment in deciding whether to accept the results of  
1270 Automated Decision Making;
- 1271 (3) implement mechanisms and safeguards, such as capacity for human  
1272 determination, that are appropriate to the use or application of the  
1273 specific Automated Decision Making given the context and purpose of  
1274 the use; and
- 1275 (4) achieve overall fairness of making predictions about an Individual  
1276 from group-level data in a given context and comply with this Section  
1277 before such predictions are relied upon or used in anyway.

1278 (b) SPECIFIC REQUIREMENTS FOR TRUSTWORTHY AND ACCOUNTABLE  
1279 AUTOMATED DECISION MAKING.<sup>40</sup>—A Covered Entity engaged in  
1280 Automated Decision Making shall develop, document, and implement  
1281 policies, processes, and procedures to ensure that—

- 1282 (1) Personal Data used in or for Automated Decision Making is labeled or  
1283 traceable to enable analysis of the Automated Decision Making and to  
1284 enable responses to an inquiry, appropriate to the context, including  
1285 the level of Processing Risk;
- 1286 (2) Automated Decision Making that makes predictions includes  
1287 indications of reliability to assist decision makers with giving the  
1288 prediction appropriate weight;
- 1289 (3) Automated Decision Making tools are designed and built to mitigate  
1290 bias in both the model and data and that proper protocols are in place


---

<sup>40</sup> Although the scope of the IAF Model with respect to Automated Decision Making and the recently released draft [EU Regulation for High Risk AI Systems](#), are different, the goals and obligations set forth in the two documents generally line up, including requirements concerning the quality of data sets used, technical documentation and record-keeping, transparency and the provision of information to users, data governance, and defined risk assessments.

- 1291 to promote transparency and accountability. Such protocols shall  
1292 address, as appropriate the—
- 1293 (A) validity of the Automated Decision Making, taking into account the  
1294 context around how the Personal Data was collected and what kind  
1295 of inference is being drawn;
  - 1296 (B) accuracy of the Automated Decision Making, taking into account the  
1297 Automated Decision Making model’s performance; and
  - 1298 (C) bias of the Automated Decision Making including examination of  
1299 potential bias at different stages of Automated Decision Making,  
1300 imperfect data quality, missing data, sampling bias, or other relevant  
1301 factors.
- 1302 (c) Policies, processes, and procedures to implement the requirements of  
1303 this Section shall be documented in order to achieve consistent  
1304 application across the Covered Entity and shall identify by name and  
1305 title the Individual authorized to approve the use of Automated  
1306 Decision Making.

1307  **Section 4.04 ACCOUNTABILITY FOR PROCESSING BY**  
1308 **SERVICE PROVIDERS AND THIRD**  
1309 **PARTIES.**

- 1310 (a) SERVICE PROVIDERS.—When a Covered Entity engages a Service  
1311 Provider to Process Personal Data, the Covered Entity shall—
- 1312 (1) exercise appropriate due diligence in the selection of the Service  
1313 Provider and take reasonable steps to maintain appropriate controls for  
1314 the Processing and security of the Personal Data;
  - 1315 (2) require the Service Provider by contract to develop, document, and  
1316 implement appropriate measures designed to meet the objectives and  
1317 requirements of this Act;
  - 1318 (3) prohibit the Service Provider by contract from Processing the Personal  
1319 Data for any purpose other than the specific purposes and legitimate  
1320 uses for which the Covered Entity Transferred such Personal Data to  
1321 the Service Provider;

- 1322 (4) require, as appropriate, managers and staff of the Service Provider to  
1323 complete education, awareness, and training programs related to  
1324 Processing; and
- 1325 (5) exercise reasonable oversight and take reasonable actions to be in  
1326 compliance with such contractual provisions, including the  
1327 implementation of an assessment process to periodically determine  
1328 whether the Service Provider has reasonable and appropriate  
1329 procedures in place to comply with this Act. The assessment process  
1330 shall reflect the particular circumstances of the Covered Entity,  
1331 including its size and complexity, the nature and scope of the Covered  
1332 Entity’s data holdings and activities with respect to Personal Data, and  
1333 the relative level of Processing Risk.
- 1334 (b) THIRD PARTIES.—A Covered Entity shall not Transfer Personal Data it  
1335 holds to a Third Party unless that Third Party is contractually bound to  
1336 meet the same Processing and security obligations as the Covered  
1337 Entity under this Act and any additional obligations to which the  
1338 Covered Entity has publicly committed. A Covered Entity shall exercise  
1339 reasonable oversight and take reasonable actions to ensure a Third  
1340 Party’s compliance with such contractual provisions.
- 1341  (c) ASSISTANCE OR SUPPORT FOR VIOLATING THIS ACT.—It shall be  
1342 unlawful and a separate violation of this Act for a Covered Entity to  
1343 provide substantial assistance to or support for the Processing of  
1344 Personal Data to any person when that Covered Entity knows or  
1345 consciously avoids knowing that the person is engaged in ongoing or  
1346 systemic acts or practices that violate this Act. Nothing in this Section  
1347 shall prohibit a Covered Entity from providing assistance or support to  
1348 a person for the sole purpose of coming into compliance with the  
1349 provisions of this Act.

1353 (d) ADDITIONAL REQUIREMENTS.—

1354 (1) A Covered Entity shall designate a qualified employee to be  
1355 responsible and accountable for each Service Provider or Third Party  
1356 and to ensure compliance with this Section of the Act.

1357 (2) A Covered Entity shall take reasonable actions to advise a Third Party  
1358 or Service Provider that relies upon or uses Automated Decision  
1359 Making created by the Covered Entity of the intended and appropriate  
1360 use of the Automated Decision Making and determine whether that  
1361 Third Party or Service Provider complies with or has policies,  
1362 processes, and procedures in place to help comply with Section 4.03.

1363  **Section 4.05 WORKFORCE ACCOUNTABILITY.**

1364 (a) DESIGNATION OF RESPONSIBLE AND ACCOUNTABLE EMPLOYEES.—A  
1365 Covered Entity shall designate one or more qualified employees who  
1366 have organization-wide responsibility and accountability for  
1367 developing, documenting, and implementing policies, processes, and  
1368 procedures to ensure compliance with this Act. Designated employees  
1369 shall exercise judgment whether their skills or expertise are sufficient to  
1370 support the demands of this section and, if these skills or expertise are  
1371 not sufficient, they shall decline to serve or obtain relevant education  
1372 and training.

1373 (b) AWARENESS AND TRAINING PROGRAMS.—A Covered Entity shall  
1374 develop, document, and implement an appropriate education,  
1375 awareness, and training program for all personnel, including employees  
1376 and independent contractors.

1377 (c) NEEDS ASSESSMENT.—A Covered Entity shall establish policies,  
1378 processes, and procedures to assess and address the hiring, training,  
1379 continuing education, and professional development needs of personnel,  
1380 including employees and independent contractors, with roles and  
1381 responsibilities related to compliance with this Act.

1382 (d) INTERNAL ENFORCEMENT.—A Covered Entity shall develop,  
1383 document, and implement policies, processes, and procedures to ensure

1384 that all personnel, including employees and independent contractors, are  
1385 held accountable for complying with organization-wide information  
1386 security and Personal Data Processing requirements and policies,  
1387 including processes and procedures for internal enforcement of the  
1388 Covered Entity’s policies and discipline for non-compliance.



**Section 4.06 OVERSIGHT: DEMONSTRATING  
TRUSTWORTHINESS, COMPLIANCE, AND ONGOING  
COMMITMENT TO RESPONSIBLE PROCESSING.**

1392 (a) INTERNAL REVIEWS.—A Covered Entity shall establish an independent  
1393 and objective internal review, audit, and assurance program to  
1394 systematically—

- 1395 (1) monitor compliance with legal obligations, including statutory,  
1396 regulatory, and contractual obligations;
- 1397 (2) monitor compliance with internal policies, processes, and procedures  
1398 and alignment with public representations;
- 1399 (3) confirm that the Covered Entity’s Processing Activities are conducted  
1400 as planned;
- 1401 (4) evaluate the effectiveness of the Covered Entity’s compliance with  
1402 this Act; and
- 1403 (5) assess whether processing impact assessments required by Article V  
1404 of this Act have been conducted with integrity and competency.

1405 (b) POTENTIAL CONFLICTS OF INTEREST.—A Covered Entity shall  
1406 develop, document, and implement reasonable and appropriate policies,  
1407 processes, and procedures to ensure that—

- 1408 (1) there is a clear separation of duties between different roles with  
1409 respect to Processing;
- 1410 (2) an accountable official responsible for approving a processing impact  
1411 assessment or approving a specific Processing Activity does not have  
1412 a private, personal, professional, financial, or other interest sufficient  
1413 to appear to influence the objective exercise of his or her official  
1414 duties; and
- 1415 (3) the oversight process is independent from the assessment process.

- 1416 (c) HIGH RISK PROCESSING ACTIVITY.—A Covered Entity engaged in  
1417 Processing that is likely to create a high or greater level of Processing  
1418 Risk shall—
- 1419 (1) create an internal data Processing review board to evaluate and  
1420 approve new Processing Activities, including Automated Decision  
1421 Making, that is reasonably likely to create a high or extreme level of  
1422 Processing Risk and assess whether the Processing has been  
1423 conducted with integrity and in full compliance with this Act; and  
1424 (2) seek external review and validation, including external audits and  
1425 certifications of policies, processes, and procedures to ensure  
1426 compliance with relevant laws, industry best practices, internal  
1427 procedures, and the requirements of this Act.
- 1428 (d) EVIDENCE OF OVERSIGHT.—A Covered Entity shall document the  
1429 internal review, audit, and assurance programs in order to demonstrate  
1430 how oversight was conducted and that, in fact, it was conducted.
- 1431 (e) SENIOR MANAGEMENT ENGAGEMENT.—A Covered Entity shall  
1432 maintain internal controls and reporting structures to ensure that  
1433 appropriate senior management officials of the Covered Entity are  
1434 involved in assessing risks, ensuring ongoing accountability, and  
1435 making decisions that implicate compliance with this Act.

1437  **Article V. PROCESSING RISK MANAGEMENT**

1438 **Section 5.01 RISK MANAGEMENT STRATEGY.<sup>41</sup>**

- 1439 (a) A Covered Entity shall develop, document, and implement a  
1440 comprehensive Processing Risk management strategy to—
- 1441 (1) manage reasonably foreseeable Processing Risk;
- 1442 (2) identify and avoid unacceptable levels of Processing Risk; and

---

<sup>41</sup> As explained in the [NIST Cybersecurity and Privacy Program](#), a well-defined risk management strategy supports a Covered Entity’s comprehensive Accountable Processing Management Program.



- 1443 (3) approve and authorize Processing or material modifications in  
1444 Processing.
- 1445 (b) The Processing Risk management strategy shall, at a minimum, include  
1446 policies, processes, and procedures designed to enable a Covered Entity  
1447 to—
- 1448 (1) identify, assess, and document the level of Processing Risk created by  
1449 a Processing Activity;
- 1450 (2) mitigate Processing Risk;
- 1451 (3) make and document an informed determination that the Processing  
1452 Risk remaining after taking steps to mitigate such risk presents an  
1453 acceptable level of Processing Risk;<sup>42</sup>
- 1454 (4) monitor Processing Risk; and
- 1455 (5) ensure the measures put in place to mitigate Processing Risk over time  
1456 are—
- 1457 (A) implemented correctly;
- 1458 (B) operating as intended; and
- 1459 (C) sufficient to ensure ongoing compliance with applicable  
1460 requirements and to manage identified and evolving Processing Risk  
1461 on a continual basis.
- 1462 (c) Processing Risk management shall be conducted as an entity-wide  
1463 activity to ensure that risk-based decision-making is applied  
1464 consistently across the Covered Entity and integrated into each aspect  
1465 of the Covered Entity’s planning and operations related to Processing.<sup>43</sup>

1466  **Section 5.02 ASSESSMENT OF PROCESSING RISK.**<sup>44</sup>

---

<sup>42</sup> “[P]rivacy risk assessments help organizations distinguish between privacy risk and compliance risk. Identifying if data processing could create problems for individuals, even when an organization may be fully compliant with applicable laws or regulations, can help with ethical decision-making in system, product, and service design or deployment. . . . This facilitates optimizing beneficial uses of data while minimizing adverse consequences for individuals’ privacy and society as a whole, as well as avoiding losses of trust that damage organizations’ reputations, slow adoption, or cause abandonment of products and services.” [NIST Privacy Framework](#) at p. 5.

<sup>43</sup> The NIST Privacy Framework recommends that the process of framing risk be conducted at an enterprise level. This process identifies executive level assumptions affecting risk assessments, risk responses, and risk monitoring; Priorities and trade-offs considered by the organization for managing risk; and organizational risk tolerance. [NIST Privacy Framework](#), Appendix D,

<sup>44</sup> The [GDPR](#), and Virginia’s new [Consumer Data Protection Act](#), also require Data Protection Assessments or Privacy Impact Assessments, which require a risk/benefit analysis of a processing activity. However, those laws fail

1467 To assess the likelihood that Adverse Processing Impact will occur as a  
1468 result of Processing, a Processing Activity, or a Processing Action and the  
1469 degree, magnitude, or potential severity of the Adverse Processing Impact,  
1470 should it occur,<sup>45</sup> a Covered Entity shall identify and inventory each piece of  
1471 data to be Processed and evaluate, at a minimum, the following 13<sup>46</sup>  
1472 factors—

(a) USE AND UTILITY.—A Covered Entity shall evaluate the use and utility  
1473 of the Personal Data alone or in combination with other data,  
1474 including—

(1) the specific, intended purpose and use for Processing;  
1476  
(2) other potential and likely uses of the Personal Data; and  
1477  
(3) potential unlawful uses and the likelihood of such uses.  
1478

(b) ADVERSE PROCESSING IMPACT.—A Covered Entity shall evaluate the  
1479 Adverse Processing Impact that may be caused by Processing Personal  
1480 Data alone or in combination with other data, considered from the  
1481 perspective of the Individual and taking into account the full range of  
1482 potential Adverse Processing Impacts identified in Section 1.03(a) of  
1483 this Act.  
1484

---

to adequately explain the risk to be evaluated and the factors to be considered when assessing risk, creating uncertainty for companies and consumers alike. The detail included here is intended to promote consistency for risk assessments and build confidence in the process. This in turn will help Covered Entities effectively and efficiently mitigate risk and meet compliance obligations. It should also promote predictable enforcement by regulators.

<sup>45</sup> The NIST Privacy Framework approach to privacy risk is to consider “*privacy events* as potential problems individuals could experience arising from system, product, or service operations with data, whether in digital or non-digital form, through a complete life cycle from data collection through disposal.” [NIST Privacy Framework](#), at p. 3. Once an organization can identify the likelihood of any given problem arising from the data processing, which the Privacy Framework refers to as a *problematic data action* it can assess the impact should the problematic data action occur.

<sup>46</sup> Nothing in Section 5.02 is new. Indeed, IAF identified an even more comprehensive set of issues and risk factors in IAF’s efforts to help companies conduct ethical data impact assessments. See, [Ethical Data Impact Assessments and Oversight Models](#) January 2019.

- 1485 (c) INDIVIDUAL MITIGATION.—A Covered Entity shall evaluate the extent  
1486 to which an Individual—
- 1487 (1) is dependent on the outcome of the Processing or Processing Activity, in  
1488 particular because, for practical or legal reasons, it is not reasonably  
1489 possible to opt-out from that outcome; and
  - 1490 (2) would be able to discover, mitigate, and fully resolve any Adverse  
1491 Processing Impact caused by Processing, taking into account the  
1492 resources that would be required for an Individual to resolve any  
1493 Adverse Processing Impact and obtain full redress.
- 1494 (d) VOLUME AND SENSITIVITY OF PERSONAL DATA.—A Covered Entity  
1495 shall evaluate the volume and sensitivity of Personal Data, including—
- 1496 (1) the extent to which the Processing involves Sensitive Personal Data;
  - 1497 (2) the number of Individuals whose Personal Data is or may be  
1498 Processed; and
  - 1499 (3) the amount of Personal Data Processed about each Individual.
- 1500 (e) IDENTIFIABILITY AND LINKABILITY.—A Covered Entity shall evaluate  
1501 identifiability and linkability of the Personal Data, including—
- 1502 (1) the extent to which a given data set is linked or linkable to an  
1503 Identifiable Individual or an Individual can be identified from a given  
1504 data set; and
  - 1505 (2) the extent to which a given data set is intended to be linked to an  
1506 Identifiable Individual at a future date or by another person.
- 1507 (f) SOURCES AND ACCURACY OF PERSONAL DATA.—A Covered Entity  
1508 shall evaluate the sources and accuracy of Personal Data, including—
- 1509 (1) the number of distinct sources of Personal Data;
  - 1510 (2) whether the Personal Data includes Provided Data, Third-Party  
1511 Provided Data, Observed Data, and Inferred Data;
  - 1512 (3) for Provided Data, the circumstances in which an Individual provided  
1513 the Personal Data;

- 1514 (4) for Third-Party Provided Data, Observed Data, or Inferred Data,  
1515 whether the Individual was or could have been aware of the Personal  
1516 Data or the Processing;
- 1517 (5) the extent to which new Personal Data is created; and
- 1518 (6) the reliability of sources and the verifiability of the accuracy of the  
1519 Personal Data for the intended purpose.
- 1520 (g) DURATION OF PROCESSING.—A Covered Entity shall evaluate the  
1521 duration of Processing, including—
- 1522 (1) the duration, period of time, or frequency of the Processing Activity,  
1523 ranging from a one-time use or single transaction to ongoing,  
1524 persistent, and systemic Processing; and
- 1525 (2) the duration and methods for which Personal Data or the results of  
1526 Processing Personal Data are stored.
- 1527 (h) REASONABLE PRIVACY EXPECTATIONS.—A Covered Entity shall  
1528 evaluate the extent to which the Personal Data—
- 1529 (1) would reasonably be considered personal, private, or of an intimate  
1530 nature under the circumstances; and
- 1531 (2) is related to activities or communications inside an Individual’s home  
1532 or equivalent location where an Individual has a reasonable  
1533 expectation of privacy, including a hotel room, rented room, locker  
1534 room, dressing room, restroom, mobile home, or interior cabin of an  
1535 Individual’s personal automobile.
- 1536 (i) EXTENT OF ACCESS, SHARING, DISCLOSURE, OR TRANSFER.—A  
1537 Covered Entity shall evaluate the extent of access, sharing, disclosure,  
1538 or Transfer, including—
- 1539 (1) the intended scope of authorized access;
- 1540 (2) the extent to which Personal Data will be Transferred to one or more  
1541 Third Parties and the category or categories of such Third Parties,  
1542 including whether the Personal Data will be Transferred to local, state,  
1543 or federal government agencies and the purpose for which such  
1544 government agency will use the Personal Data;

- 1545 (3) intended public disclosure of Personal Data or widespread  
1546 dissemination; and
- 1547 (4) the extent to which Personal Data will be Transferred to one or more  
1548 jurisdictions outside the United States.<sup>47</sup>
- 1549 (j) VULNERABLE POPULATIONS.—A Covered Entity shall evaluate the  
1550 extent to which the Processing targets or otherwise involves an  
1551 identifiable or inferred vulnerability or potentially vulnerable  
1552 population or the Adverse Processing Impact arising from Processing  
1553 disproportionately affects a vulnerable population. For the purpose of  
1554 this Act, vulnerable populations include children<sup>48</sup>; the elderly;  
1555 Individuals with a serious health condition, impairment, cognitive  
1556 deficiency, or disability; victims of certain crimes; deployed members  
1557 of the military and their families; communities recovering from crisis or  
1558 disaster; or groups facing undue economic hardship.
- 1559 (k) RELIANCE ON AUTOMATED DECISION MAKING.—A Covered Entity  
1560 shall evaluate the extent to which a Covered Entity uses or relies upon  
1561 Automated Decision Making and the level of confidence that the  
1562 Automated Decision Making is sufficiently accurate and appropriate for  
1563 the intended use.
- 1564 (l) CONSISTENT WITH THE CONTEXT.—A Covered Entity shall evaluate  
1565 the extent to which the Processing is Consistent with the Context of the  
1566 relationship between the Individual and the Covered Entity.

---

<sup>47</sup> In contrast with EU law, Covered Entities are not expected to verify, on a case-by-case basis, whether the law of the third country of destination ensures an adequate level of protection for Personal Data. See, e.g., [GDPR](#) Article 45(1). On the other hand, a Covered Entity should assess the potential risk of adverse processing impact to Individuals or specific categories of Individuals when Transferring Personal Data outside of the United States. For example, in some jurisdictions simply being a member of a particular minority group or expressing certain opinions could create a significant risk of harm. A Covered Entity should consider this type of risk before transferring Personal Data to such a jurisdiction. Here again, context is highly relevant, and a general rule cannot be applied to all circumstances. This provision should not in any way be interpreted as a data localization requirement.

<sup>48</sup> IAF believes that children’s privacy is a critically important issue but chose not to address this issue in the IAF Model. There are many ongoing initiatives related to children’s privacy. IAF has not conducted research in this area and does not have any particular expertise with respect to processing data about children. IAF anticipates that children’s privacy would be addressed in a separate law or be incorporated into a law based on the framework codified in the IAF Model.

1567 (m) LEGAL OBLIGATIONS.—A Covered Entity shall evaluate all statutory,  
1568 regulatory, contractual, and other legal obligations or restrictions that  
1569 may apply to the Processing.

1570 **Section 5.03 CATEGORIZATION OF PROCESSING RISK.**

1571 (a) LEVELS OF RISK.—When conducting a processing impact assessment, a  
1572 Covered Entity shall categorize the level of Processing Risk as very  
1573 low, low, moderate, high, or extreme.

1574 (b) For the purpose of this Act, the term “extreme” refers to a severe, dire  
1575 or catastrophic Adverse Processing Impact that results in—

1576 (1) loss of life;

1577 (2) life threatening or incapacitating injury, illness, or health condition;

1578 (3) restriction of freedom, including incarceration, quarantine, involuntary  
1579 commitment, limitations on travel or movement, or forced relocation;

1580 (4) separation or isolation from family members; or

1581 (5) infringement of a right guaranteed by the Constitution of the United  
1582 States.

1583 (c) When classifying risk, a Covered Entity shall select the higher risk  
1584 categorization if there is doubt as to the appropriate classification  
1585 between two risk levels.

1586 (d) No Covered Entity shall be held liable for a violation of this Act solely  
1587 for incorrectly categorizing the level of risk for a particular Processing  
1588 Activity if the Covered Entity establishes by a preponderance of the  
1589 evidence that the Covered Entity maintained reasonable policies,  
1590 processes, and procedures to identify, assess, document, and mitigate  
1591 risk as required by Article V of this Act.

1592 **Section 5.04 PROCESSING IMPACT ASSESSMENTS.<sup>49</sup>**

---

<sup>49</sup> The IAF believes that a decision is not risk-based unless there is a measurement of the risks and benefits at issue and the integrity of the assessment is demonstrable to others. Risk/benefit decisions are not always intuitive. They require assessments that identify: the parties that might be impacted by the use of data, how they might be impacted, and whether the risks and benefits are mapped to the people, groups of people and society. Decisions must be explainable to others based on objective measures.

- 1593 (a) WHEN TO CONDUCT.—A Covered Entity shall conduct and document  
1594 a processing impact assessment when, at a minimum, Processing or a  
1595 Processing Activity—
- 1596 (1) is reasonably likely to create a moderate or greater level of Processing  
1597 Risk;
  - 1598 (2) involves new or novel methods of Automated Decision Making or an  
1599 application of Automated Decision Making that is not widely in use in  
1600 commerce; or
  - 1601 (3) is conducted for a legitimate use as defined in Sections 2.01(b)(8),  
1602 2.01(b)(9), or 2.01(b)(10) of this Act unless the Covered Entity  
1603 determines with a reasonable degree of certainty that the Processing or  
1604 Processing Activity will create no more than a very low level of  
1605 Processing Risk.
- 1606 (b) REQUIRED ANALYSIS.— At a minimum, a processing impact  
1607 assessment shall analyze and explain—
- 1608 (1) the purpose, mission, business needs, and objectives of the Processing  
1609 Activity;
  - 1610 (2) the functional needs or capabilities of the Processing Activity;
  - 1611 (3) the Adverse Processing Impact that may be created by the Processing  
1612 Activity, taking into account the full range of potential Adverse  
1613 Processing Impact identified in Section 1.03(a) of this Act;
  - 1614 (4) the level of Processing Risk that may be created by the Processing  
1615 Activity, taking into account the 13 factors identified in Section  
1616 5.02;<sup>50</sup>
  - 1617 (5) the administrative, technical, and physical controls, safeguards, and  
1618 other measures implemented to mitigate Processing Risk and other

---

<sup>50</sup> NIST explains that a risk assessment should “[d]etermin[e] the likelihood and impact of adverse effects on individuals arising from the processing of [personal data].” NIST [Security and Privacy Controls for Information Systems and Organizations](#), 800-53, Revision 5 (September 2020), at p. 240.

- 1619 risk throughout the lifecycle of the Personal Data and Processing  
1620 Activity;
- 1621 (6) the level of Processing Risk remaining after all practicable and  
1622 reasonable measures are taken to mitigate Processing Risk;
- 1623 (7) the Covered Entity’s decision that the Processing Risk remaining  
1624 presents an acceptable level of Processing Risk;
- 1625 (8) the Benefits to Individuals or Competition; and
- 1626 (9) the Covered Entity’s decision to authorize and approve Processing and  
1627 the basis for that decision, including the factors that support  
1628 Processing despite the designated level of Processing Risk.
- 1629 (c) TIMING.—
- 1630 (1) A processing impact assessment shall be completed and documented  
1631 before a Covered Entity begins Processing.
- 1632 (2) Processing impact assessments shall be reviewed and updated on an  
1633 ongoing basis to ensure they are accurate and current pursuant to a  
1634 review schedule determined and documented by the Covered Entity as  
1635 part of the Covered Entity’s risk management program.
- 1636 (d) ACCOUNTABLE OFFICIAL. —A Covered Entity shall designate one or  
1637 more qualified employees who are authorized to accept risk. A  
1638 processing impact assessment shall identify the employee who  
1639 approved the level of Processing Risk and authorized Processing.

1640  **Section 5.05 ENHANCED PROCESSING IMPACT**  
1641 **ASSESSMENT TO ASSESS IMPLICATIONS**  
1642 **OF AUTOMATED DECISION MAKING.**

- 1643 (a) A Covered Entity shall conduct an enhanced processing impact  
1644 assessment before the Covered Entity relies on Automated Decision  
1645 Making unless the Covered Entity concludes with a reasonable degree  
1646 of certainty that the any Processing which relies upon Automated  
1647 Decision Making is unlikely to create a moderate or greater level of  
1648 Processing Risk.
- 1649 (b) An enhanced processing impact assessment shall, in addition to the  
1650 requirements set forth in Section 5.04 of this Act—



- 1651 (1) enable a relevant employee or other person to see how and why an  
1652 Automated Decision Making model produced the specific outcome;  
1653 (2) provide attestation that Automated Decision Making models and  
1654 insights have been tested, to the extent practicable, for accuracy and  
1655 predictability;  
1656 (3) identify the specific Individual or body who has ultimate decision-  
1657 making authority for the use of Automated Decision Making or  
1658 reliance upon Automated Decision Making;  
1659 (4) identify potentially biased data sets and assess the desirability of  
1660 modifying or not using the data set;  
1661 (5) detect and proactively mitigate bias, including potential bias that may  
1662 develop or evolve as models learn or adapt to new experiences or  
1663 stimuli;  
1664 (6) detect and proactively mitigate discrimination;  
1665 (7) determine the useful life of each Automated Decision Making output;  
1666 (8) explain how the Covered Entity considered and implemented the  
1667 requirements set forth in Sections 4.03 and 4.04 of this Act; and  
1668 (9) confirm that an appropriate mechanism has been established to enable  
1669 an Individual to challenge an adverse outcome created by the use or  
1670 application of Automated Decision Making as required by Section  
1671 3.05(b) of this Act.

1672  **Section 5.06 BAD FAITH.**

1673 With respect to Processing that begins after the effective date of this Act, it  
1674 shall be unlawful, and an independent and separate violation of this Act to—

- 1675 (a) misrepresent, expressly or by implication, that a processing impact  
1676 assessment or enhanced processing impact assessment was completed  
1677 before the commencement of Processing;  
1678 (b) produce a processing impact assessment or enhanced processing impact  
1679 assessment for the purpose of justifying and documenting a decision  
1680 that was previously made without evaluating Processing Risk as  
1681 required by this Act; or

1682 (c) omit material facts from a privacy impact assessment that are likely to  
1683 impact or influence the analysis required by Sections 5.04 or 5.05 of  
1684 this Act.

1685 **Section 5.07 RULEMAKING.**

1686 The Commission shall, within 18 months of enactment of this Act and in  
1687 accordance with section 553 of title 5, United States Code, promulgate  
1688 regulations with respect to the assessment and categorization of Processing  
1689 Risk consistent with the purposes of this Act.

1690

1691 **Article VI. ENFORCEMENT BY COMMISSION AND STATE**  
1692 **ATTORNEYS GENERAL**

1693 **Section 6.01 ENFORCEMENT BY COMMISSION.<sup>51</sup>**

1694 (a) IN GENERAL.—A violation of this Act or any regulation prescribed  
1695 under this Act shall be treated as a violation of a rule under section 18  
1696 of the Federal Trade Commission Act (15 U.S.C. 57a) regarding unfair  
1697 or deceptive acts or practices. Except where the Commission has been  
1698 expressly granted additional authority under this Act, the Commission  
1699 shall enforce this Act in the same manner, by the same means, and with  
1700 the same jurisdiction, powers, and duties as though all applicable terms  
1701 and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et  
1702 seq.) were incorporated into and made a part of this Act.

1703

1704

1705 (b) CIVIL PENALTIES.—

1706 (1) Any Covered Entity, other than a non-profit organization as defined in  
1707 Section 1.03(h)(1)(C) of this Act, who violates the specific provisions  
1708 of this Act as set forth in Section 6.01(b)(3) below or any regulation  
1709 prescribed under this Act shall be subject to the penalties and entitled

---

<sup>51</sup> Strong, consistent, and flexible enforcement is essential to make sure that Covered Entities comply. There is bipartisan consensus that the limited tools available to the FTC today are inadequate to address the evolving consumer protection, privacy and data security challenges of the digital economy.

1710 to the privileges and immunities provided in the Federal Trade  
1711 Commission Act as though all applicable terms and provisions of the  
1712 Federal Trade Commission Act were incorporated into and made a  
1713 part of this Act.

1714 (2) In considering whether a civil penalty is in the public interest, the  
1715 Commission shall consider—

1716 (A) the gravity of the violation, including whether the act or omission for  
1717 which such penalty is assessed involved fraud, deceit, manipulation,  
1718 bad faith, or deliberate or reckless disregard of a regulatory  
1719 requirement;

1720 (B) the severity of Adverse Processing Impact to Individuals resulting  
1721 either directly or indirectly from such act or omission;

1722 (C) the level of Processing Risk created by the relevant Processing  
1723 Activity and the extent to which the Covered Entity took reasonable  
1724 steps to mitigate the Processing Risk;

1725 (D) the history of previous violations or unlawful conduct;

1726 (E) the size, financial resources, and good faith of the Covered Entity  
1727 charged;

1728 (F) the need to deter such Covered Entity from committing such acts or  
1729 omissions; and

1730 (G) such other matters as justice may require.

1731 (3) VIOLATIONS SUBJECT TO CIVIL PENALTIES.—

1732 (A) Upon the effective date of this Act, a Covered Entity may be subject  
1733 to civil penalties for violations of Sections 2.01(a), 2.01(c), 2.02(a),  
1734 2.02(c), 2.03, 3.01(a), 3.01(b), 3.02, 3.04(a)3.04(b), 3.04(c), 3.05(a),  
1735 3.06,4.01(b), 4.02(c), 4.03, 4.04, 4.05, and 4.06(d).

1736 (B) Upon the effective date of this Act, a Covered Entity engaged in  
1737 Processing that creates a high or extreme level of Processing Risk  
1738 may be subject to civil penalties for violations of Sections 4.01(c),  
1739 4.01(d), 4.02(d), and 5.06.

1740 (C) In addition to the civil penalties provided for in 6.02(b)(1) and  
1741 6.02(b)(3) above, beginning 2 years after the effective date of this  
1742 Act, a Covered Entity may be subject to civil penalties for violations  
1743 of each Section in Articles III, IV, and IV.

1744 (4) CIVIL PENALTY CAP.—

1745 (A) Notwithstanding Sections 6.01(b)(1) and (3) above, no civil penalty  
1746 shall be imposed under this Act in excess of \$1,000,000,000 arising  
1747 out of the same acts or omissions.

1748 (B) The civil penalty cap set forth in this Section does not apply to—

1749 (i) civil penalties related to a violation of a Commission order  
1750 or otherwise imposed pursuant to statutes or regulations enforced  
1751 by the Commission; and

1752 (ii) acts or omissions that constitute independent and separate  
1753 violations of this Act as set forth in Sections 2.03, 3.02(e),  
1754 3.04(b)(2), 3.07(b)(3), 4.04(c), and 5.06 of this Act.

1755 (c) EQUITABLE RELIEF.—In any action or proceeding brought or instituted  
1756 by the Commission under this Act, the Commission may seek, and any  
1757 Federal court using its full equitable powers may grant, such equitable  
1758 relief that may be appropriate or necessary to obtain monetary or other  
1759 relief for past harm or injury, to prevent further violations of this Act, or  
1760 as otherwise may be in the public interest. Such equitable remedies may  
1761 include—

1762 (1) temporary restraining order;

1763 (2) preliminary or permanent injunction;

1764 (3) cease-and-desist order;

1765 (4) rescission or reformation of contracts;

1766 (5) refund of money or return of property;

1767 (6) redress, restitution, or disgorgement of profits;

1768 (7) public notification requiring that a Covered Entity make accurate  
1769 information available through disclosures, direct notification or

1770 education, or publish educational information reasonably related to the  
1771 violations;

1772 (8) other remedies reasonably related to the unlawful practices conducted  
1773 by the Covered Entity, as may be necessary to provide complete relief  
1774 in light of the purposes of this Act or prevent future violations of this  
1775 Act; and

1776 (9) such other and further equitable relief as the court deems  
1777 appropriate.<sup>52</sup>

1778 (d) LIABILITY AND ACCOUNTABILITY FOR INDIVIDUALS IN POSITIONS OF  
1779 AUTHORITY.—

1780 (1) An Individual may be liable for a violation of this Act upon a showing  
1781 that the Individual—

1782 (A) had authority to direct or control the Covered Entity’s acts or  
1783 practices; and

1784 (B) had actual knowledge of the Covered Entity’s improper acts or  
1785 practices; or

1786 (C) exercised reckless, sustained, and systematic failure to exercise  
1787 oversight.

1788 (2) An Individual shall not be liable for civil penalties under this Act  
1789 unless—

1790 (A) the Individual knowingly violated this Act; and  
1791 (B) the Individual’s unlawful conduct created a high or extreme level of  
1792 Processing Risk and caused significant Adverse Processing Impact.

1793 (e) ENFORCEMENT AUTHORITY PRESERVED.—Nothing in this Section  
1794 shall be construed to affect any authority of the Commission under any  
1795 other provision of this Act or other law. Remedies provided in this  
1796 Section are in addition to, and not in lieu of, any other remedy or right  
1797 of action otherwise provided by this Act or any other provision of law.

---

<sup>52</sup> This provision explicitly provides the FTC with the authority to seek equitable remedies, including monetary relief. Among other things, this provision restores the FTC with the authorities struck down by the US Supreme Court in [AMG Capital Management, LLC v. FTC](#), and eliminates any further ambiguities in the [FTC Act](#), 15 U.S.C. § 45 et seq., with respect to the FTC’s authority to seek equitable remedies.

1798 (f) STAY OF ENFORCEMENT.—The Commission may stay enforcement of  
1799 one or more specific provisions of this Act for no more than 1 year after  
1800 the effective date upon finding that such stay is in the public interest.  
1801 The stay shall apply to all entities that are authorized to enforce this  
1802 Act.<sup>53</sup>

1803 (g) JURISDICTION OVER COMMON CARRIERS AND NON-PROFIT  
1804 ORGANIZATIONS.—Notwithstanding Sections 4, 5(a)(2), or 6 of the  
1805 Federal Trade Commission Act (15 U.S.C. 44, 45(a)(2), 46) or any  
1806 jurisdictional limitation of the Commission, the Commission shall  
1807 enforce this Act with respect to—

- 1808 (1) common carriers subject to the Communications Act of 1934 (47  
1809 U.S.C. 151 et seq.); and  
1810 (2) organizations not organized to carry on business for their own profit  
1811 or that of their members, as defined in Section 1.03(h)(1)(C) of this  
1812 Act.

1813 (h) INDEPENDENT LITIGATING AUTHORITY.—The Commission is  
1814 authorized to litigate cases, by its own attorneys, before any federal  
1815 court or tribunal within the judicial branch of the United States in order  
1816 to enforce the provisions of this Act and rules thereunder, and  
1817 includes authority to commence, defend, intervene in, or appeal any  
1818 action, suit, or proceeding to which the Commission is a party; enter  
1819 and enforce orders issued for violations of this Act; litigate court orders  
1820 related to proceedings to enforce this Act; and argue appeals of such  
1821 orders or court decisions related to enforcement of this Act.

1822

1823  **Section 6.02 ENFORCEMENT BY STATE ATTORNEYS**  
1824 **GENERAL.**

1825 (a) In any case in which the attorney general of a State has reason to  
1826 believe that an interest of the residents of that State has been or is

---

<sup>53</sup> This provision authorizes the FTC to extend the enforcement grace period from 2 years to 3 years in the event the FTC does not complete the rulemaking on time or for other reasons in the public interest.

1827 adversely affected by any person who violates this Act, the attorney  
1828 general of the State, as *parens patriae*, may bring a civil action on behalf  
1829 of the residents of the State in an appropriate district court of the United  
1830 States to—

- 1831 (1) enjoin further violation of this Act by the defendant;
- 1832 (2) compel compliance with this Act;
- 1833 (3) obtain damages, restitution, or other compensation on behalf of the  
1834 residents of the State;
- 1835 (4) obtain civil penalties in the amount determined and consistent with the  
1836 requirements under Section 6.01(b) above; and
- 1837 (5) obtain such other relief as the court using its full equitable  
1838 powers deems appropriate.

1839 (b) The attorney general of a State shall notify the Commission in writing  
1840 of any civil action prior to initiating such civil action. Upon receiving  
1841 notice with respect to a civil action, the Commission may—

- 1842 (1) intervene in such action; and
- 1843 (2) upon intervening—
  - 1844 (A) be heard on all matters arising in such civil action; and
  - 1845 (B) file petitions for appeal of a decision in such action.

1846 (c) **PREEMPTIVE ACTION BY COMMISSION.**—If the Commission institutes a  
1847 civil action for violation of this Act or a regulation promulgated under  
1848 this Act, no attorney general of a State may bring a civil action against  
1849 any defendant named in the complaint of the Commission for the  
1850 violations of this Act or a regulation promulgated pursuant to this Act  
1851 alleged in the complaint.



**Section 6.03 SAFE HARBOR PROGRAMS FOR  
RESPONSIBLE AND ACCOUNTABLE  
COVERED ENTITIES.**

1852 (a) **IN GENERAL.**—Industry groups or other persons may apply to the  
1853 Commission for approval of self-regulatory programs (“safe harbor  
1854 programs”) that provide guidance to Covered Entities on how to  
1855 comply with requirements and obligations of this Act in the context of  
1856  
1857  
1858

1859 specific industries, subsectors, technologies, or Processing Activities. A  
1860 safe harbor program may address compliance with the entire Act or  
1861 may be narrowly tailored to address compliance with one or more  
1862 specified provisions of the Act.

1863 (b) CRITERIA FOR APPROVAL OF PROGRAM GUIDELINES.—To be eligible  
1864 for approval by the Commission, a safe harbor program shall, at a  
1865 minimum—

1866 (1) specify clear and enforceable requirements for a Covered Entity  
1867 participating in the safe harbor program that provide substantially the  
1868 same or greater protections as those contained in the relevant  
1869 provisions of this Act;

1870 (2) require each participating Covered Entity to post in a prominent place  
1871 a clear and conspicuous public attestation of compliance;

1872 (3) require a process for the independent assessment of a participating  
1873 Covered Entity’s compliance with the safe harbor program prior to  
1874 attestation and on an annual basis; and

1875 (4) take meaningful action for non-compliance with the safe harbor  
1876 program or with relevant provisions of this Act by any participating  
1877 Covered Entity.

1878 (c) EFFECT OF APPROVAL.—A Covered Entity that complies with a safe  
1879 harbor program approved by the Commission shall be deemed to be in  
1880 compliance with the provisions of this Act addressed by such program.

1881 (d) EFFECT OF NON-COMPLIANCE.— A Covered Entity that has certified  
1882 compliance with an approved safe harbor program and is found not to  
1883 be in compliance with such program by the Commission shall be  
1884 considered to be in violation of the section 5 of the Federal Trade  
1885 Commission Act (15 U.S.C. § 45) prohibition on unfair or deceptive  
1886 acts or practices.

1887 (e) RULEMAKING.—The Commission shall, within 1 year of enactment of  
1888 this Act and in accordance with section 553 of title 5, United States  
1889 Code, promulgate regulations to implement this Section of the Act. The



1890 regulations by the Commission shall, at a minimum, identify the  
1891 procedures for such safe harbor programs to be submitted to the  
1892 Commission for approval and the criteria by which the Commission  
1893 shall review, reject, or approve the proposed program in whole or in  
1894 part.

1895 **Section 6.04 SAFE HARBOR FOR ACCOUNTABLE**  
1896 **SMALL BUSINESS AND NON-PROFIT**  
1897 **ORGANIZATIONS.**

- 1898 (a) A Covered Entity shall not be subject to enforcement as set forth in  
1899 Article VI of this Act where the Covered Entity—  
1900 (1) is engaged in interstate commerce and independently owned and  
1901 operated; or  
1902 (2) operates across states and meets the definition of non-profit set forth  
1903 in section 501 of title 26, United States Code; and  
1904 (3) Processes Personal Data of fewer than 50,000 Individuals in any 12-  
1905 month period;  
1906 (4) does not derive 50% or more of its annual revenue from selling or  
1907 licensing Personal Data; and  
1908 (5) engages only in Processing that is likely to create no more than a  
1909 moderate level of Processing Risk.  
1910 (b) MINIMUM REQUIREMENTS.—In order to be subject to the safe harbor, a  
1911 Covered Entity shall make a legally enforceable public representation  
1912 that the Covered Entity meets the criteria of Section 6.04(a) and has  
1913 taken reasonable steps to confirm that the representation is and remains  
1914 true as long as the Covered Entity relies on the safe harbor.

1915 **Section 6.05 ACCOUNTABILITY REPORTS AND**  
1916 **ASSESSMENTS.**

- 1917 (a) AUTHORITY TO OBTAIN INFORMATION AND DOCUMENTS.—  
1918 (1) In addition to its existing authority pursuant to the Federal Trade  
1919 Commission Act and other laws enforced by the Commission,  
1920 including this Act, the Commission shall have the authority to require,  
1921 by special orders, a Covered Entity, other than a non-profit

1922 organization as defined in Section 1.03(h)(1)(C) of this Act, to file  
1923 with the Commission, in such form as the Commission may prescribe,  
1924 reports or answers in writing to specific questions, furnishing to the  
1925 Commission such information as it may require as to the Covered  
1926 Entity's—

- 1927 (A) business operations;
- 1928 (B) Processing Activities; and
- 1929 (C) policies, processes, and procedures developed, documented, and  
1930 implemented by the Covered Entity to meet the requirements of this  
1931 Act.

1932 (2) The Commission may seek such information, as it deems necessary to  
1933 ensure that commercial practices are consistent with the requirements  
1934 of this Act, assess compliance, determine whether a violation of law  
1935 exists, gather information necessary to support the report to Congress  
1936 as required by Section 7.04 of this Act, or for other reports to  
1937 Congress or the Executive Branch. Information sought must be  
1938 reasonably relevant to the Commission's mission, the purposes of this  
1939 Act, and in the public interest. Special orders issued pursuant to this  
1940 Section shall be reasonable and shall not impose an undue burden on a  
1941 Covered Entity.

- 1942 (3) Reports and answers shall be made under oath, or otherwise, as the  
1943 Commission may prescribe, and shall be filed with the Commission  
1944 within such reasonable period as the Commission may prescribe.
- 1945 (4) The Commission's authority to obtain information pursuant to this  
1946 Section shall not be subject to the Paperwork Reduction Act (44  
1947 U.S.C. 3501-3520).

1948 (b) REVIEW OF RECORDS.—All final records, documents, or assessments  
1949 required to be made and kept by a Covered Entity pursuant to this Act  
1950 are subject at any time, or from time to time, to such reasonable  
1951 periodic, special, or other review by representatives of the Commission  
1952 as the Commission deems necessary or appropriate in the public

1953 interest, for the protection of Individuals, or otherwise in furtherance of  
1954 the purposes of this Act.

1955 (1) PROCEDURES.—A Covered Entity shall have the same right to  
1956 challenge an order issued pursuant to this Section and seek judicial  
1957 review of a decision by the Commission as provided for Commission  
1958 orders issued pursuant to Section 6(b) of the Federal Trade  
1959 Commission Act (15 U.S.C. 46(b)).

1960  **Section 6.06 IMPLEMENTING REGULATIONS TO**  
1961 **SUPPORT ACCOUNTABILITY.**

1962 (a) AUTHORITY.—The Commission shall, in accordance with section 553  
1963 of title 5, United States Code, promulgate regulations to carry out the  
1964 purposes of this Act.

1965 (b) AUTHORITY TO GRANT EXCLUSIONS.—In promulgating rules under  
1966 this Act, the Commission may implement such additional exclusions  
1967 from this Act as the Commission considers consistent with the purposes  
1968 of this Act and in the public interest.

1969 (c) CRITERIA FOR ISSUANCE OF RULES.—

1970 (1) In promulgating regulations, the Commission shall consider—

1971 (A) the potential Processing Risk to Individuals and society arising from  
1972 a particular act or practice;

1973 (B) the potential benefits to Individuals and competition arising from the  
1974 particular act or practice; and

1975 (C) that compliance with such regulations must allow for flexibility in  
1976 implementation and be reasonable and appropriate for a Covered  
1977 Entity taking into account—

1978 (i) the size, resources, and complexity of the Covered Entity;

1979 (ii) the nature and scope of the Covered Entity’s Processing Activities;

1980 (iii) the potential level of Processing Risk created by such Processing;  
1981 and

1982 (iv) the burden on a Covered Entity that is a non-profit organization as  
1983 defined in Section 1.03(h)(1)(C) of this Act.

- 1984 (d) TECHNOLOGY NEUTRAL.—In promulgating such regulations, the
- 1985 Commission shall not require the deployment or use of any specific
- 1986 products or technologies, including any specific computer software or
- 1987 hardware, nor prescribe or otherwise require that computer software or
- 1988 hardware products or services be designed, developed, or manufactured
- 1989 in a particular manner.
- 1990 (e) MANDATORY REVIEW.—The Commission shall evaluate the need for
- 1991 modifications to the regulations promulgated to implement this Act as
- 1992 warranted and, at a minimum, every 3 years.
- 1993

1994  **Article VII. COMMISSION EDUCATION, GUIDANCE, OUTREACH,**

1995 **AND REPORTS**

1996 **Section 7.01 CONSUMER EDUCATION.**

1997 In order to protect Individuals’ personal information and to ensure that

1998 Individuals have the confidence to take advantage of the many benefits of

1999 products offered in the marketplace, the Commission shall publish resources

2000 to educate Individuals with respect to—

- 2001 (a) the various ways an Individual may interact with Processing as well as
- 2002 devices and technology that enable Processing including the collection
- 2003 of Personal Data;
- 2004 (b) the potential benefits and risks, including risk of Adverse Processing
- 2005 Impact, that may be associated with Processing in order to help
- 2006 Individuals make more informed decisions;
- 2007 (c) helping Individuals compare the Processing Activities of different
- 2008 digital products and services; and
- 2009 (d) helping Individuals understand their options with respect to Processing
- 2010 by a Covered Entity provided for by this Act.

2011  **Section 7.02 GUIDANCE AND OUTREACH FOR**

2012 **COVERED ENTITIES.**

- 2013 (a) GUIDANCE.—The Commission shall publish guidance, training
- 2014 materials, proposed best practices, and other resources designed to
- 2015 assist Covered Entities with coming into compliance with obligations

2016 under this Act, taking into account that the requirements of this Act are  
2017 intended to be flexible and scalable to accommodate the range in types  
2018 and sizes of Covered Entities that must comply with the provisions of  
2019 this Act.

2020 (b) SMALL BUSINESS SUPPORT.—Recognizing that small businesses make  
2021 up a large and vital segment of the U.S. economy, the Commission shall  
2022 develop and implement guidance and resources specifically designed to  
2023 help small businesses meet their obligations under this Act and shall  
2024 undertake outreach efforts to ensure that small businesses are aware of  
2025 their obligations under the Act and the resources available to support  
2026 small businesses.

2027 (c) The Commission shall establish a mechanism for a Covered Entity to  
2028 submit an inquiry to the Commission regarding compliance with this  
2029 Act. To the extent practicable and in the public interest, the  
2030 Commission shall make available to the public the Commission’s  
2031 responses to such inquiries and shall take such inquiries into account  
2032 when developing guidance and educational materials for Covered  
2033 Entities. Responses may take the form of a Commission staff opinion  
2034 letter or such other form as the Commission determines meets the  
2035 objectives of this Section and purposes of this Act.



**Section 7.03 INTERNATIONAL COOPERATION FOR  
THE PROTECTION OF PERSONAL DATA.<sup>54</sup>**

2038 The Commission shall, consistent with its current authorities, endeavor to  
2039 cooperate and coordinate with foreign agencies and provide such agencies  
2040 with information regarding this Act to foster—

2041 (a) understanding of the protections for Personal Data and Individuals  
2042 under this Act;<sup>55</sup>

---

<sup>54</sup> In an effort to develop a framework that will be interoperable with legal regimes around the world, IAF looked to principles published by non-governmental organizations such as the OECD and APEC, as well as legal frameworks in the EU, Canada, Australia and Asia. Many concepts have been ported from GDPR, including the definitions of personal data and processing.

<sup>55</sup> Accountability is a basic tenet of 21st century data protection law and governance across the globe. It is referenced explicitly [GDPR](#), Canada’s [Personal Information Protection and Electronic Documents Act](#) (PIPEDA), the [APEC Privacy Framework, Advisory Guidelines](#) on Key Concepts in the new Singaporean Personal Data

- 2043 (b) consistency in the interpretation and enforcement for the protection of  
2044 Personal Data;
- 2045 (c) cooperation and convergence toward best practices with respect to  
2046 Processing covered by this Act; and
- 2047 (d) timely evaluation of complaints with respect to alleged violations of this  
2048 Act, subject to rules and restrictions as the Commission may determine,  
2049 from Individuals regardless of country of residency.

2050 **Section 7.04 REPORT.**

2051 Not later than 3 years after the date of enactment of this Act, the  
2052 Commission shall transmit to Congress a report describing the  
2053 Commission's use of and experience with the authority granted by this Act,  
2054 along with any recommendations for revisions to the Act or additional  
2055 legislation. The report shall include—

- 2056 (a) the number of complaints related to the Processing of Personal Data or  
2057 alleged violations of this Act received by the Commission;
- 2058 (b) the number of investigations initiated by the Commission related to the  
2059 Processing of Personal Data and suspected violations of this Act;
- 2060 (c) the number of enforcement actions initiated by the Commission for  
2061 alleged violations of this Act and a summary of such enforcement  
2062 actions;
- 2063 (d) the Commission's efforts to coordinate with State Attorneys General  
2064 regarding enforcement of this Act;
- 2065 (e) the status of any rulemaking proceedings undertaken pursuant to this  
2066 Act;
- 2067 (f) the Commission's efforts to provide guidance to Covered Entities,  
2068 including small sized Covered Entities as provided for in Section  
2069 7.02(b) of this Act;
- 2070 (g) the Commission's efforts to provide education to Individuals as  
2071 provided for in Section 7.01 of this Act;

---

Protection Act, and draft legislation introduced in Canada, [An Act to Enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act](#), as an update to PIPEDA.

- 2072 (h) the Commission’s efforts to support the effective implementation and  
2073 application of the safe harbor provisions of this Act, including approval  
2074 of codes of conduct, as provided for in Section 6.03 of this Act;  
2075 (i) the Commission’s exercise of its authority under Section 6.04 of this  
2076 Act to undertake assessment reviews; and  
2077 (j) Commission resources allocated to the implementation and enforcement  
2078 of this Act and an assessment of the adequacy of such resources.  
2079

2080  **Article VIII. COMMISSION RESOURCES AND AUTHORIZATION OF**  
2081 **APPROPRIATIONS**

2082 **Section 8.01 APPOINTMENT OF ADDITIONAL**  
2083 **PERSONNEL.**

- 2084 (a) Notwithstanding any other provision of law, the Chair of the  
2085 Commission may, without regard to the civil service laws (including  
2086 regulations), appoint additional personnel for the purpose of enforcing  
2087 this Act and otherwise meeting the Commission’s obligations under this  
2088 Act, including—  
2089 (1) 250 additional personnel in attorney positions; and  
2090 (2) 250 additional personnel in project management, technical, and  
2091 administrative support positions.  
2092 (b) COMPENSATION.<sup>56</sup>—Notwithstanding any otherwise applicable  
2093 provision of title 5, United States Code, concerning compensation,  
2094 including the provisions of chapter 51 and chapter 53, the following  
2095 provisions shall apply with respect to employees appointed pursuant to  
2096 this Act or employed by the Commission for the purpose of enforcing  
2097 this Act and otherwise meeting the obligations under this Act—

---

<sup>56</sup> This provision would bring the salaries of FTC staff in line with equivalent staff at financial regulators, which is approximately 30% more than other federal government employees. This is necessary for the FTC to be able to compete for resources with technology companies and law firms. This provision is based on a proposal by former FTC Chairman William E. Kavocic, [Jones, Alison and Kovacic, William E., The Institutions of U.S. Antitrust Enforcement: Comments for the U.S. House Judiciary Committee on Possible Competition Policy Reforms \(June 4, 2020\).](#)

- 2098 (1) the rates of basic pay for all employees hired pursuant to paragraph (a)  
2099 may be set and adjusted by the Chair of the Commission;  
2100 (2) the Chair of the Commission shall at all times provide compensation  
2101 (including benefits) to each class of employees that, at a minimum, are  
2102 comparable to the compensation and benefits then being provided by  
2103 the Board of Governors for the corresponding class of employees; and  
2104 (3) all such employees shall be compensated (including benefits) on terms  
2105 and conditions that are consistent with the terms and conditions set  
2106 forth in section 11(l) of the Federal Reserve Act (12 U.S.C. 248(l)).

2107  **Section 8.02 AUTHORITY TO ESTABLISH NEW BUREAU**  
2108 **OR OFFICE.**

2109 The attorneys and support personnel appointed pursuant to Section 8.01 of  
2110 this Act shall be assigned to the Bureau of Consumer Protection or such  
2111 other bureau or office as the Chair may create, taking into account—

- 2112 (a) the efficient and effective application of Commission resources;  
2113 (b) avoidance of duplicative functions;  
2114 (c) impact on the Commission’s ability to carry out its dual mission of  
2115 protecting consumers and promoting competition; and  
2116 (d) the public interest.

2117  **Section 8.03 AUTHORIZATION OF APPROPRIATIONS.**

2118 There is authorized to be appropriated to the Commission such sums as may  
2119 be necessary to carry out this Act.  
2120

2121 **Article IX. PREEMPTION<sup>57</sup>**

2122 **Section 9.01 PREEMPTION.**

2123 For a Covered Entity subject to this Act, the provisions of this Act shall  
2124 preempt any civil provisions of the law of any State or political subdivision

---

<sup>57</sup> IAF generally supports the concept of preemption. Consistent national privacy standards would benefit both individuals and industry. Article IX provides an example of language that may help policymakers address this complex issue but should not necessarily be interpreted as language endorsed by IAF. IAF believes that the substantive provisions of any framework should be addressed first so that the scope of the bill can inform discussions regarding preemption and related matters.



2125 of a State to the degree they are focused on the reduction of Processing Risk  
2126 through the regulation of Personal Data Processing Activities.

2127 **Section 9.02 EFFECT ON OTHER LAWS.**

2128 (a) CONSUMER PROTECTION LAWS.—Except as provided in Section 9.01,  
2129 this Act shall not be construed to limit the enforcement or the bringing  
2130 of a claim pursuant to any State consumer protection law by an attorney  
2131 general of a State, other than to the extent to which those laws regulate  
2132 Personal Data collection and Processing.

2133 (b) PROTECTION OF CERTAIN STATE LAW.—Nothing in this Act shall be  
2134 construed to preempt the applicability of—

2135 (1) the constitutional, trespass, contract, data breach notification, or tort  
2136 law of any state, other than to the degree such laws are substantially  
2137 intended to govern Personal Data collection and Processing;

2138 (2) any other state law to the extent that the law relates to acts of fraud,  
2139 wiretapping, or the protection of social security numbers;

2140 (3) any state law to the extent it provides additional provisions to  
2141 specifically regulate the Covered Entities as defined in the Health  
2142 Insurance Portability and Accountability Act of 1996 (Public Law  
2143 104–91), the Family Educational Rights and Privacy Act (Public Law  
2144 93–380), the Fair Credit Reporting Act (Public Law 91–508) or the  
2145 Financial Services Modernization Act of 1999 (Public Law 106–102);  
2146 or

2147 (4) private contracts based on any state law that require a party to provide  
2148 additional or greater protections to an Individual than does this Act.

2149 (c) PRESERVATION OF COMMISSION AUTHORITY.—Nothing in this Act  
2150 shall be construed to in any way limit the authority of the Commission  
2151 under any other provision of law.

2152 (d) FCC AUTHORITY.—Insofar as any provision of the Communications  
2153 Act of 1934 (47 U.S.C. 151 et seq.), including section 222 of the  
2154 Communications Act of 1934 (47 U.S.C. 222), or any regulations  
2155 promulgated under such Act, apply to any person subject to this Act

2156 with respect to privacy policies, terms of service, and practices covered  
2157 by this Act, such provision of the Communications Act of 1934 or such  
2158 regulations shall have no force or effect, unless such regulations pertain  
2159 to emergency services.

2160 (e) TREATMENT OF COVERED ENTITIES GOVERNED BY OTHER FEDERAL  
2161 LAW.—Covered entities subject to the Health Insurance Portability and  
2162 Accountability Act of 1996 (Public Law 104–91), the Family  
2163 Educational Rights and Privacy Act (Public Law 93–380), the Fair  
2164 Credit Reporting Act (Public Law 91–508), or the Financial Services  
2165 Modernization Act of 1999 (Public Law 106–102), are excluded from  
2166 the provisions of this Act to the degree specific uses of Personal Data  
2167 are covered by the relevant provisions of those laws.

2168  **Section 9.03 GOVERNMENT ACCOUNTABILITY OFFICE**  
2169 **STUDY AND REPORT.**

2170 Not later than 3 years after the effective date of this Act, the Comptroller  
2171 General of the United States shall submit to the President and Congress a  
2172 report that surveys federal privacy and security laws that—

- 2173 (a) identifies inconsistencies between this Act and other federal privacy  
2174 and security laws; and
- 2175 (b) provides recommendations to modify, amend, or rescind provisions of  
2176 this Act or provisions of other federal laws in order to avoid or  
2177 eliminate inconsistent, contradictory, duplicative, or outdated legal  
2178 requirements that may no longer be relevant or necessary to protect  
2179 consumers in light of this Act, rules thereunder, and changing  
2180 technological and economic trends.

2182 **Article X. EFFECTIVE DATE AND SAVINGS CLAUSE.**

2183 **Section 10.01 EFFECTIVE DATE.<sup>58</sup>**

---

<sup>58</sup> Timeline for Implementation:

Year 0: Date of Enactment

18 months: FTC completes mandatory rulemaking regarding risk assessments

18 months: FTC completes mandatory rulemaking regarding the opt out of transfers of personal data

Year 2: FTC completes mandatory rulemaking regarding codes of conduct

2184 The provisions of this Act that apply to Covered Entities shall apply  
2185 beginning on or after the date that is 2 years from the date of enactment of  
2186 this Act.

2187 **Section 10.02 NO RETROACTIVE APPLICABILITY.**

2188 This Act shall not apply to—

2189 (a) any conduct that occurred before the effective date under Section 10.01;

2190 or

2191 (b) any Personal Data collected or created before the date of enactment of  
2192 this Act.

2193 **Section 10.03 SAVINGS CLAUSE.**

2194 If any provision of this Act, an amendment made by this Act, or the  
2195 application of such provision or amendment to any person or circumstance  
2196 is held to be unconstitutional, the remainder of this Act, the amendments  
2197 made by this Act, and the application of the provisions of such to any  
2198 person or circumstance shall not be affected thereby.

2199

---

Year 2: FTC completes mandatory rulemaking regarding for Article III  
Year 2: FTC completes mandatory rulemaking regarding categories of data to be disclosed  
Year 3: Effective Date - law in effect and enforceable by FTC with limitations on civil penalties  
Year 4: Expiration of optional 1 year stay of enforcement by FTC.  
Year 5: All civil penalty provisions in effect (non-profits remain exempt)  
Year 6: GAO Study regarding conflicts among federal privacy laws  
Year 6: First FTC study regarding enforcement and compliance with Act  
Year 6: First mandatory rule review by FTC